UNIVERSITY OF TECHNOLOGY SYDNEY
Faculty of Engineering and Information Technology

Performance analysis of Unmanned Aerial Vehicles-enabled Wireless Networks

by

Xin Yuan

A Thesis Submitted
in Partial Fulfillment of the
Requirements for the Degree

Doctor of Philosophy

Sydney, Australia

2020

Certificate of Authorship/Originality

I, Xin Yuan declare that this thesis, is submitted in fulfilment of the requirements for the award of doctor of philosophy, in the Faculty of Engineering and Information Technology at the University of Technology Sydney. This thesis is wholly my own work unless otherwise reference or acknowledged. In addition, I certify that all information sources and literature used are indicated in the thesis. I certify that the work in this thesis has not previously been submitted for a degree nor has it been submitted as part of the requirements for a degree except as fully acknowledged within the text. This thesis is the result of a research candidature jointly delivered with Beijing University of Posts and Telecommunications as part of a Collaborative Doctoral Research Degree. This research is supported by the Australian Government Research Training Program.

Signature: Production Note:
Signature removed prior to publication.

Date: 02/02/2020

ABSTRACT

Performance analysis of Unmanned Aerial Vehicles-enabled Wireless Networks

by

Xin Yuan

As an indispensable part of mobile communication systems, Unmanned Aerial Vehicles (UAVs) can be leveraged to complement terrestrial networks by providing coverage to areas where infrastructures are scarce. Equipped with self-navigation and strong automation, UAVs have extensive applications to environmental monitoring, disaster recovery, search and rescue, owing to their excellent agility and autonomy. As a result, an increasing demand arises for ubiquitous connectivity and reliable communication for data exchange between UAVs, and between UAVs and ground stations. Since UAVs operate in three-dimensional (3D) space with strong manoeuvrability, random trajectories and wireless propagation environment can pose significant challenges to the study on coverage and capacity of UAV networks. On the other hand, UAVs are increasingly posing threats to information security. UAVs can be potentially used to eavesdrop and jam wireless transmissions between legitimate terrestrial transceivers. It is of practical interest to understand the robustness of terrestrial wireless communications under exposure to new threats from aerial adversaries. This thesis studies the coverage and capacity, including secure coverage and secrecy capacity, of UAV-enabled wireless networks with UAVs flying under 3D random trajectories based on stochastic geometry and measure convergence theory. The detailed contributions of this thesis are summarised as:

- Capacity analysis of UAV networks under random trajectories. We geometrically derive probability distributions of UAV-to-UAV distances and closed-form bounds for the capacity can be obtained by exploiting the Jensen's in-

equality. We extrapolate the idea to dense UAV networks and analyse the impact of network densification and imperfect channel state information on the capacity.

- Connectivity analysis of uncoordinated UAV swarms. New closed-form bounds are derived for the outage probability of individual UAVs, and broadcast connectivity of each UAV which evaluates the reliability of broadcast across the swarm. The qualifying conditions of the bounds on 3D coverage and impact of ground interference on the outage are identified.

- Secure connectivity analysis in UAV networks. We propose a trust model based on UAVs' behaviour and mobility pattern and characteristics of inter-UAV channels. We derive analytical expressions of both physical and secure connectivity probabilities with/without considering Doppler shift.

- Secrecy capacity analysis against aerial eavesdroppers. We analyse ergodic and ϵ-outage secrecy capacities of ground link in the presence of cooperative aerial eavesdroppers. The "cut-off" density of eavesdroppers under which the secrecy capacities vanish is identified. By decoupling the analysis of random trajectories from random channel fading, closed-form approximations with almost sure convergence to the secrecy capacities are devised.

Dissertation directed by Professor Ren Ping Liu, Associate Professor Andrew Zhang, and Dr. Wei Ni
School of Electrical and Data Engineering

Acknowledgements

Throughout the writing of this thesis, I have received a great deal of support and assistance. I would first like to thank my principal supervisor, Prof. Ren Ping Liu, whose expertise was invaluable in the formulating of the research topic and methodology in particular. I appreciate all his contributions of time, ideas, and funding to make my PhD experience productive.

I owe my deepest gratitude to my co-supervisor, Dr. Wei Ni, for his scientific advice and knowledge and many insightful discussions and suggestions. He is my primary resource for getting my science questions answered and was instrumental in helping me crank out this thesis. I also would like to thank my co-supervisor A/Prof. Andrew Zhang, for his patience, encouragement and insightful comments on my research.

I especially thank my supervisor, Prof. Zhiyong Feng, from Beijing University of Posts and Telecommunications (BUPT), for her support, guidance, encouragement, and technical comments through all years of my research. Special thanks to BUPT, Beijing, China, and University of Technology Sydney (UTS) for providing a scholarship and other financial support for my study and research.

I also thank my friends for providing a happy distraction to rest my mind outside of my research. Finally, I would like to express my deep and sincere gratitude to my parents for their encouragement, constant support and unconditional love, they have kept me moving forward even in tough times. This journey would not have been possible if not for them, and I dedicate this milestone to them.

Xin Yuan

Sydney, Australia, 2020.

List of Publications

Journal Papers

J-1. **X. Yuan**, Z. Feng, W. Ni, R. P. Liu, J. Zhang, and W. Xu,"Secrecy Performance of Terrestrial Radio Links under Collaborative Aerial Eavesdropping," *IEEE Transactions on Information Forensics and Security*, June 2019.

J-2. **X. Yuan**, Z. Feng, W. Ni, Z. Wei, R. P. Liu, and J. Zhang, "Secrecy Capacity Analysis against Aerial Eavesdropper," *IEEE Transactions on Communications*, July 2019.

J-3. **X. Yuan**, Z. Feng, W. Xu, W. Ni, J. Zhang Z. Wei, and R. P. Liu, "Capacity Analysis of UAV Communications: Cases of Random Trajectories," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 8, pp. 7564-7576, Aug. 2018.

J-4. **X. Yuan**, Z. Feng, W. Xu, Z. Wei, and R. P. Liu, "Secure Connectivity Analysis in Unmanned Aerial Vehicle Networks," *Frontiers of Information Technology & Electronic Engineering*, 19, 409-422, 2018.

J-5. Z. Wei, H. Wu, **X. Yuan**, S. Huang and Z. Feng, "Achievable Capacity Scaling Laws of Three-Dimensional Wireless Social Networks," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 3, pp. 2671-2685, March 2018.

J-6. S. Huang, Z. Wei, **X. Yuan**, Z. Feng and P. Zhang, "Performance Characterization of Machine-to-Machine Networks With Energy Harvesting and Social-Aware Relays," *IEEE Access*, vol. 5, pp. 13297-13307, 2017.

J-7. Z. Wei, Z. Wang, **X. Yuan**, H. Wu and Z. Feng, "Information Density-based Energy-limited Capacity of Ad Hoc Networks," *International Journal of Distributed Sensor Networks*, 2018, 14(4): 1550147718773242.

Conference Papers

C-1. **X. Yuan**, Z. Wei, Z. Feng, Q. Zhang and W. Li, "Throughput Scaling Laws of Hybrid Wireless Networks with Proximity Preference," *IEEE Wireless Communications and Networking Conference*, Doha, 2016, pp. 1-6.

C-2. **X. Yuan**, Z. Wei, Z. Feng and W. Xu, "Trust Connectivity Analysis in Overlaid Unmanned Aerial Vehicle Networks," 17th International Symposium on Communications and Information Technologies (ISCIT), Cairns, QLD, 2017, pp. 1-6.

C-4. Z. Wei, Z. Feng, **X. Yuan**, X. Feng, Q. Zhang and X. Wang, "The Achievable Capacity Scaling Laws of 3D Cognitive Radio Networks," *IEEE International Conference on Communications (ICC)*, Kuala Lumpur, 2016, pp. 1-6.

C-5. S. Liu, Z. Wei, Z. Guo, **X. Yuan** and Z. Feng, "Performance Analysis of UAVs Assisted Data Collection in Wireless Sensor Networks," *IEEE 87th Vehicular Technology Conference (VTC Spring)*, Porto, 2018, pp. 1-5.

C-6. J. Shang, W. Xu, C. Lee, **X. Yuan**, P. Zhang, and J. Lin "Delay Estimation of UAV Communications Based on Fountain Codes," *IEEE 30th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, 2019.

Contents

Certificate ii

Abstract iii

Acknowledgments v

List of Publications vi

List of Figures xiii

Abbreviation xvii

Notation xx

1 Introduction 1

1.1 Background 1

1.2 Research Problems and Challenges 6

1.3 Research Objectives and Contributions 8

1.3.1 Research Objectives 8

1.3.2 Research Contributions 8

1.4 Thesis Organization 10

2 Literature Review 12

2.1 UAV-enabled Wireless Network 12

2.2 Performance analysis of Wireless Networks 13

2.2.1 Performance analysis of Traditional wireless Networks 13

2.2.2 Performance analysis of UAV-enabled Wireless Networks . . . 14

2.3 Physical Layer Security 15
2.3.1 Physical Layer Security in Traditional Wireless Networks . . . 15
2.3.2 Physical Layer Security in UAV-enabled Wireless Networks . . 16
2.3.3 Performance Metrics for Physical Layer Security 17

3 Capacity Analysis of UAV-enabled Wireless Networks 19

3.1 Introduction 19
3.2 System Model and Problem Formulation 20
3.2.1 System Model 20
3.2.2 Definitions of Performance Metrics 22
3.3 Link Capacity of UAV Communications 25
3.3.1 U2U Link with 3D Random Trajectories 25
3.3.2 U2U Link with 2D Random Trajectories 27
3.3.3 U2G Link with 3D Random Trajectories 28
3.4 Network Densification and Relay 30
3.4.1 Direct Link 30
3.4.2 Relayed Link 32
3.5 Simulation and Evaluation 33
3.6 Discussions and Extensions 37
3.6.1 Interference from the Ground Station 37
3.6.2 Imperfect CSI at the Receiver 40
3.7 Conclusion 41
3.8 Appendix 42
3.8.1 Proof of the convexity of C_{erg1} with respect to l. 42
3.8.2 Proof of Theorem 1. 43

3.8.3 Proof of Corollary 1. 46

3.8.4 Proof of Corollary 2. 48

4 Connectivity Analysis of UAV-enabled Wireless Networks 50

4.1 Introduction 50

4.2 System Model and Problem Formulation 51

4.2.1 Outage Probability 52

4.3 Connectivity of the UAV Swarms 55

4.3.1 Connectivity of Individual UAVs 56

4.3.2 Broadcast Connectivity of the UAV Swarm 58

4.4 Connectivity of the UAV Swarms under the ground Interference 60

4.4.1 Outage Probability under Interference from Ground Transmitter 60

4.4.2 Connectivity analysis 63

4.5 Simulation and Evaluation 64

4.5.1 Connectivity of individual UAVs 65

4.5.2 Broadcast Connectivity of the UAV Swarm 70

4.6 Conclusion 70

4.7 Appendices 71

4.7.1 Proof of Theorem 2. 71

4.7.2 Proof of Theorem 3. 72

4.7.3 Proof of $\mathcal{X} - \mathbb{E}[\mathcal{X}] \longrightarrow 0$. 73

4.7.4 Proof of Theorem 5. 74

4.7.5 Proof of Corollary 3. 76

5 Secure Connectivity Analysis of UAV-enabled Wireless Networks 80

5.1 Introduction 80

5.2 System Model and Definitions 83

5.2.1 Network Model 84

5.2.2 Definition of Secure Links 84

5.3 Trust Modeling and Calculation 85

5.3.1 Efficient Hierarchical Trust Model 85

5.3.2 Trust Calculation 87

5.4 Secure Connectivity Analysis of UAV Networks under Doppler Shifts . 94

5.4.1 Physical Connection in UAV Networks 94

5.4.2 Secure Connectivity Analysis 99

5.5 Simulation and Evaluation 99

5.5.1 Performance of the Trust Model 100

5.5.2 Physical Connectivity Probability 103

5.5.3 Secure Connectivity Probability 106

5.6 Conclusion 107

6 Secrecy Performance Analysis of Terrestrial Radio Links against Aerial Eavesdroppers 109

6.1 Introduction 109

6.2 System Model 110

6.2.1 Mobility Model 110

6.2.2 Channel Model 113

6.3 Average Achievable Secrecy Rate in the Presence of an Aerial Eavesdropper . . . 116
6.3.1 Ergodic Secrecy Rate . . . 116
6.3.2 Average ϵ-Outage Secrecy Rate . . . 119
6.3.3 Ergodic and Outage Secrecy Rates under Practical UAV Channel Model . . . 121
6.4 Simulation and Evaluation . . . 123
6.5 Conclusion . . . 130
6.6 Appendix . . . 131
6.6.1 Proof of (6.1) – (6.3) . . . 131
6.6.2 Proof of Lemma 5 . . . 133
6.6.3 Proof of $\mathbb{E}\left[\log_2\left(\frac{\mathcal{X}}{\mathcal{Y}}\right)\right] \xrightarrow{a.s.} \log_2\left(\frac{\mathbb{E}[\mathcal{X}]}{\mathbb{E}[\mathcal{Y}]}\right)$. . . . 134
6.6.4 Proof of Theorem 6 . . . 135
6.6.5 Proof of Lemma 6 . . . 138
6.6.6 Proof of Theorem 7 . . . 141
6.6.7 Proof of (6.23). . . . 142

7 Conclusion and Future Work **146**

Bibliography **149**

List of Figures

1.1 Forecast curves for the number of UAS by the US Department of Defense and public agencies. 2

1.2 Illustration of an Air-space-ground integrated information network . . 5

3.1 Illustration on a pair of autonomous UAVs flying random 3D trajectories with smooth turns. 20

3.2 Two UAVs in the spherical region (Special case: UAV 1 is located on the surface of the 3D spherical region). 25

3.3 Two UAVs in a 2D disk (Special case: UAV 1 is located on the boundary of the disk). 27

3.4 The ergodic capacity vs. radius, with the Rician factor $K = 5$ dB, $P = 0.1$ W. 34

3.5 The outage capacity vs. radius, with the Rician factor $K = 5$ dB, $P = 0.1$ W, and $\vartheta_{\text{th}} = 10$ dB. 35

3.6 The outage capacity vs. SNR threshold, with the Rician factor $K = 5$ dB, $P = 0.1$ W, and $r_s = 500$ m. 36

3.7 The ergodic capacity vs. SNR threshold, with the Rician factor $K = 5$ dB, $P = 0.01$ W, and $\vartheta_{\text{th}} = 0$ dB. 36

3.8 SINR vs. radius, with $P = 0.1$ W, $P_I = 0.1$ W, and $\alpha = 3$. 40

4.1 A UAV swarm flies autonomously and randomly within a 3D sphere. 51

4.2 The curve of $\tilde{Q}(l)$ vs. distance l, where $K = 5$ dB, $\rho_{\text{th}} = 5$ dB, $P = 0.1$ W and $\sigma^2 = -70, -80$ dBm. 53

4.3 Two UAVs in the spherical region (Special case: UAV 1 is located on the boundary of the spherical region). 56

4.4 The outage probability of an arbitrary UAV vs. the number of UAVs, N, under different Rician factors, where $r = 500$ m, $\rho_{\text{th}} = 5$ dB, and $\alpha_I = 3.5$. 65

4.5 The outage probability in the presence of interference from the ground transmitter vs. the outage probability in the absence of interference from the ground transmitter under different α_I, where $r = 500$, $N = 50$, $K_I = 0$, and $\alpha = 3$. 66

4.6 The outage probability of an arbitrary UAV vs. the number of UAVs under different SNR/SINR thresholds, where $K = K_I = 0$ and $r = 500$ m. 67

4.7 The outage probability of an arbitrary UAV vs. the transmit power of UAVs for different values of SNR threshold, where $r = 500$ m, $N = 50$, $\alpha = 3$,$\alpha_I = 3.5$, and the Rician factor is $K = 0$. 68

4.8 The outage probability of an arbitrary UAV vs. the radius of the sphere r, under different total numbers of UAVs, where the Rician factor $K = 0$, $P = 0.1$ W and $\rho_{\text{th}} = 5$ dB. 68

4.9 The outage probability between the furthest pair of UAVs in the UAV swarm. 69

5.1 An illustration of a UAV network with a trust link. Here, solid lines and dotted lines denote physical links and trust links, respectively. . . 83

5.2 Secure link abstracted from UAV Networks in Fig. 5.1. (1) physical link; (b) trust link; (c) secure link. 84

5.3 The structure of trust model 86

5.4 An illustration of the Oblate Spheroid Model 95

5.5 Communication packets are higher than the threshold 101

5.6 Communication packets are lower than the threshold 101

5.7 Influence of the weight value 102

5.8 Influence of trust update time interval 103

5.9 Robustness against mobility 104

5.10 Physical connectivity probability P_{phy} vs. Communication range r_{th} . 104

5.11 Physical connectivity probability P_{phy} vs. Speed V 105

5.12 Connectivity probability vs. Communication range r_{th} 106

5.13 Connectivity probability vs. Communication range r_{th} 106

6.1 The system of interest, where there is a pair of legitimate transmitter and receiver on the ground, and an aerial eavesdropper flying within the transmission range of the transmitter. The eavesdropper follows the ST mobility model. 111

6.2 The scenario of a bidirectional ground link, where the aerial eavesdropper flies within the overlapping coverage region of both the legitimate ground nodes. 124

6.3 The ergodic secrecy rate vs. the radius of the eavesdropper's flight region, r, under different values of path loss, α_e, where $L = 200$ m, and $\alpha = 3$. 125

6.4 The ergodic secrecy rate vs. $\frac{\alpha_e}{\alpha}$, in the presence of an aerial eavesdropper under different values of path loss exponent, α_e, where $\alpha = 4$. 126

6.5 The ϵ-outage secrecy rate vs. the radius of the eavesdropper's flight region, r, under different values of both path loss exponent and Rician factors, where $\alpha = 3$, $L = 200$ m, and $\epsilon = 0.1$. 127

6.6 The ϵ-outage secrecy rate vs. the outage probability, ϵ, in the presence of an aerial eavesdropper flying in 3D spherical spaces, where $L = 200$ m, $r = 800$ m, and $\alpha = 3$. 128

6.7 The ϵ-outage secrecy rate vs. $\frac{\alpha_e}{\alpha}$, under different values of both target secrecy rate and Rician factor. 129

6.8 The secrecy rates (Scenario 1) under different $\alpha_{\frac{\pi}{2}}$ values, where $L = 200$ m, $K = 0$, $K_e = 10$ dB, and $\alpha_0 = 3$. 130

6.9 Geometric manipulation for the proof of (6.1) – (6.3). 131

6.10 Geometric interpretation for the evaluation of l_e 142

Abbreviation

a.s. - Almost sure

i.i.d. - Independent and identically distributed

CDF - Cumulative distribution function

PDF - Probability of Density

2DPSK - Binary DPSK

2D: Two-dimensional

3D: Three-dimensional

5G - The 5th Generation mobile communication system

6G - The 6th Generation mobile communication system

A2A - Air-to-air

A2G - Air-to-ground

AA - Azimuth angle

AWGN - Additive white Gaussian noise

BER - Bit error rate

BS - Base station

BPP - Binomial point process

BPSK - Binary Phase Shift Keying

CDMA: Code Division Multiple Access

CoMP: Coordinated Multi-Point

CSMA/CA - Carrier-sense multiple access with collision avoidance

CSI: Channel State Information

CQI: Channel Quality Indicator

D2D: Device to Device

DoF - Degree-of-freedom

DPSK - Differential Phase Shift Keying

M2M: Machine to Machine

MIMO: Multi input multi output

E2E: End-to-end

EA - Elevation angle

EHTM - Efficient hierarchical trust model

FDD: Frequency Division Duplex

FDMA: Frequency Division Multiple Access

G2G: Ground-to-ground

G2U: Ground-to-UAV

JP: Joint Processing

LTE: Long Term Evolution

LTE-A: Long Term Evolution-Advanced

LoS: Line-of-sight

MAC: Medium access control

MANET: Mobile Ad Hoc Network

MIMO: Multiple Input Multiple Output

MISO: Multiple Input Single Out

MMSE: Minimum Mean Square Error

MRC: Mobile Ad Hoc Network

NLoS: Non line-of-sight

PER: Packet error rate

PMF: Probability Mass Function

PGF: Probability Generating Functional

PLL: Phase-locked loop

PLR: packet loss rate

PPP: Poisson Point Process

PRR: Packet Receiving Ratio

QoS: Quality of Service

RF: Radio Frequency

RMS: Root-mean-square

RSRP: Reference Signal Received Power

RSSI: Received Signal Strength Indicator

SC: Selection combining

SINR: Signal to Interference plus Noise Ratio

SNR: Signal-to-noise ratio

SON: Self-Organized Network

SRCM: Semi-Random Circular Movement

ST:Smooth Turn

SVD: Singular value decomposition

TDD: Time Division Duplex

TDMA: Time Division Multiple Access

MTC: Machine Type Communication

ICIC: Inter-Cell Interference Coordination

WiMAX: Worldwide Interoperability for Microwave Access

WSN: Wireless Sensor Networks

U2G: UAV-to-Ground

UAV: Unmanned Aerial Vehicles

VANET: Vehicular Ad hoc Network

ZF: Zero Forcing

Nomenclature and Notation

Capital letters denote matrices.

Lower-case alphabets denote column vectors.

$(\cdot)^T$ denotes the transpose operation.

$(\cdot)^*$ denotes the complex conjugate operation.

$(\cdot)^{\mathrm{H}}$ denotes the conjugate transpose operation.

I_n is the identity matrix of dimension $n \times n$.

0_n is the zero matrix of dimension $n \times n$.

$\mathbb{R}$, $\mathbb{R}^+$ denote the field of real numbers, and the set of positive reals, respectively.

$(\cdot)^+$ denotes $\max\{\cdot, 0\}$.

$|\cdot|$ denotes the modulo operation.

$\mathbb{E}[\cdot]$ denotes the expectation operation.

$f(\cdot)$ denotes the probability distribution function.

$F(\cdot)$ denotes the cumulative distribution function.

$\Pr(\cdot)$ denotes the probability function.

$\frac{\partial y}{\partial x}$ denotes the first order partial derivative of y to x.

$\frac{\partial^2 y}{\partial x^2}$ denotes the second order partial derivative of y to x.

$\mathbf{1}(\cdot)$ denotes the indicator function.

$B(a, b)$ denotes the Beta function with parameter a and b.

$\beta(\cdot; \cdot, \cdot)$ denotes the incomplete beta function.

$\Gamma(\cdot)$ denotes the Γ function.

$\gamma(a, b) = \int_0^b e^{-t} t^{a-1} dt$ denotes the incomplete gamma function.

${}_2F_1(a, b; c; z) = \sum_{n=0}^{\infty} \frac{(a)_n (b)_n}{(c)_n} \cdot \frac{z^n}{n!}$ denotes the Gaussian hypergeometric function.

Chapter 1

Introduction

This chapter mainly introduces the research background, discusses the challenges and problems of the UAV-enabled wireless networks, and presents the objectives, the contributions and the structure of this thesis.

1.1 Background

According to the US Defense Report "Unmanned aircraft systems roadmap 2005-2030 [1]", it is predicted that there will be 70,000 drones in the United States by 2035, as shown in Fig. 1.1. Unmanned Aerial Vehicle (UAV) system can provide wireless network coverage for remote areas, and can also serve as an effective relay for information transmission between terrestrial communication networks and satellite communication networks [2, 3]. UAV may play a central role in providing network services recovery in a disaster-stricken region, enhancing public safety networks, or handling other emergency situations. In particular, UAV-aided base station can be regarded as an important complement to fifth generation (5G) cellular networks [4]. The landscape of 5G radio access networks is expected to seamlessly and ubiquitously connect everything, and support at least 1000-fold traffic volumes, 100 billion connected wireless devices, and diversified requirements on reliability, latency, battery lifetime, etc, as opposed to current fourth generation (4G) cellular networks. As a result, UAVs are identified as an important component of 5G/B5G wireless technologies [5]. The UAVs have the advantages of small size, flexibility, and rapid deployment, and can be widely used in military and civilian fields [6, 7, 8, 9]. Military use of UAVs is more than 25 years mainly consisting of border surveillance,

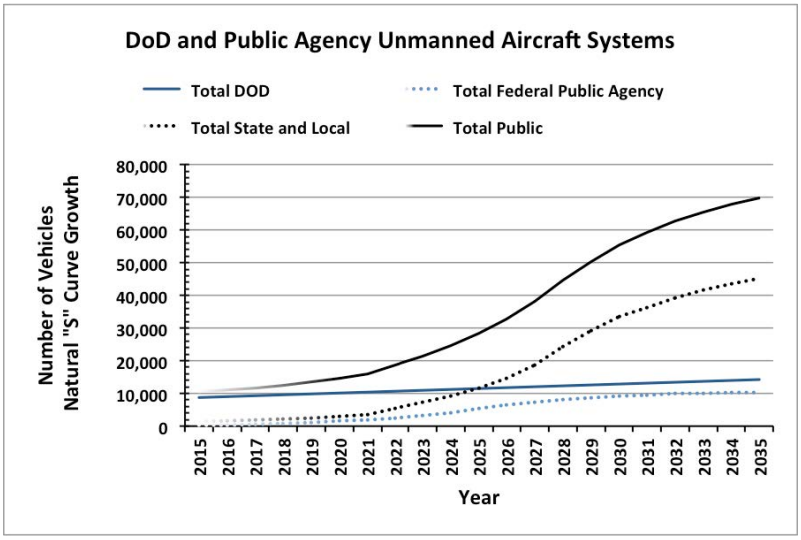


Figure 1.1 : Forecast curves for the number of UAS by the US Department of Defense and public agencies [1].

reconnaissance and strikes. For the civilian use by some public institutions, such as police, public safety and transportation management, UAVs can provide timely warnings of disasters and assist in accelerating rescue and recovery operations when public communication networks are broken [10].

The UAV is limited by its size, capacity (such as battery capacity), payload and flight time, a single UAV sometimes cannot meet the task requirement. However, multiple UAV collaborations can accomplish tasks efficiently and successfully [11]. Teams of UAVs can be deployed, for instance, as aerial base stations to provide service to disaster-affected areas or as an aerial sensor network, collecting data in large areas. Such teams can have the potential to perform tasks that go beyond the individual capabilities of the small UAVs. Specifically, the multi-UAV system has the advantages of less time required to perform tasks and a wide operation coverage.

However, the collaboration in multi-UAV system raises many challenges and problems, especially when the multi-UAV system autonomously performs missions. Although the multi-UAV system is able to change behaviors to handle unexpected events, it is difficult for them to plan and execute different actions with little or no

human interactions [12]. Communication and networking can realize interoperability between UAVs, and are essential to enable team behavior, coordinate multiple UAVs, and achieve autonomous UAV networks [10]. It is very likely that high-performance wireless links and connectivity in three-dimensional (3D) space will be required for several applications with data delivery under certain quality-of-service (QoS) demands [7].

A Wireless Ad Hoc Network (WANET) does not need to pre-configure the network infrastructure and has the characteristics of easy deployment, self-organization, and dynamic topology. It is widely used in scenarios such as search and rescue without communication infrastructure and can realize multiple UAV collaboration. Flying Ad Hoc Network (FANET) can be defined as a new form of MANET in which the nodes are UAVs [13]. Based on its definition, a single-UAV system cannot form a FANET, which is only valid for multi-UAV systems. FANET can also be classified as a subclass of Vehicular Ad Hoc Network (VANETs). The FANET has similar features to MANET and VANET, and these similarities encourage researchers to explore and discover the applicability of existing work in MANET and VANET, but the work in these areas does not adequately address the unique characteristics of the problems in the FANET.

The multi-UAV system, classified as FANET [13], not only has the characteristics of no control center and self-organization, but also has the unique characteristics, including node mobility, node density, radio propagation model, topology change, and power consumption. The main advantages of the multi-UAV system, or UAV-enabled wireless networks (or UAV networks for short), are summarized as follows [13]:

- Reduce task completion time. The use of multi-UAV systems (or UAV networks) can effectively reduce the execution time of tasks such as reconnais-

sance, surveillance, search and rescue. The more the number of drones, the faster the task can be performed.

- Extending the scalability of multi-UAV operation. A multi-UAV system established based on an infrastructure (such as a ground station or a satellite) can only operate within the communication coverage area of the infrastructure. In the case of a UAV cannot communicate with the infrastructure, its operation fails. On the other hand, the UAV network is based on the UAV-to-UAV (U2U) data links instead of UAV-to-infrastructure (U2I) data links, and it can extend the operation area in a self-organizing manner. Even if a UAV in the network cannot be connected to the infrastructure, it can still operate by establishing a multi-hop communication link.

- Reliable multi-UAV communication. The communication between the UAVs is susceptible to the surrounding environment, such as obstacles including the ground buildings and mountains, which can attenuate radio signal propagation. The multi-UAV networks can be self-organized to connect the UAVs and effectively improve the operation efficiency. When a UAV is interrupted, the self-organization of the UAV network can be used to maintain the network connectivity through relaying from other UAVs. The self-organization of the UAV network can reduce the dependence on the infrastructure and thereby enhancing the network reliability.

- UAV swarms. Small UAVs are very light and have limited payload capacity. Despite their restricted capabilities, the swarm behavior of the multiple UAVs can complete complex missions. The swarm behavior requires communication between the UAVs to achieve mutual coordination and avoid collisions. The self-organization between UAVs can effectively prevent collisions between UAVs and enables effective coordination to successfully accomplish tasks.

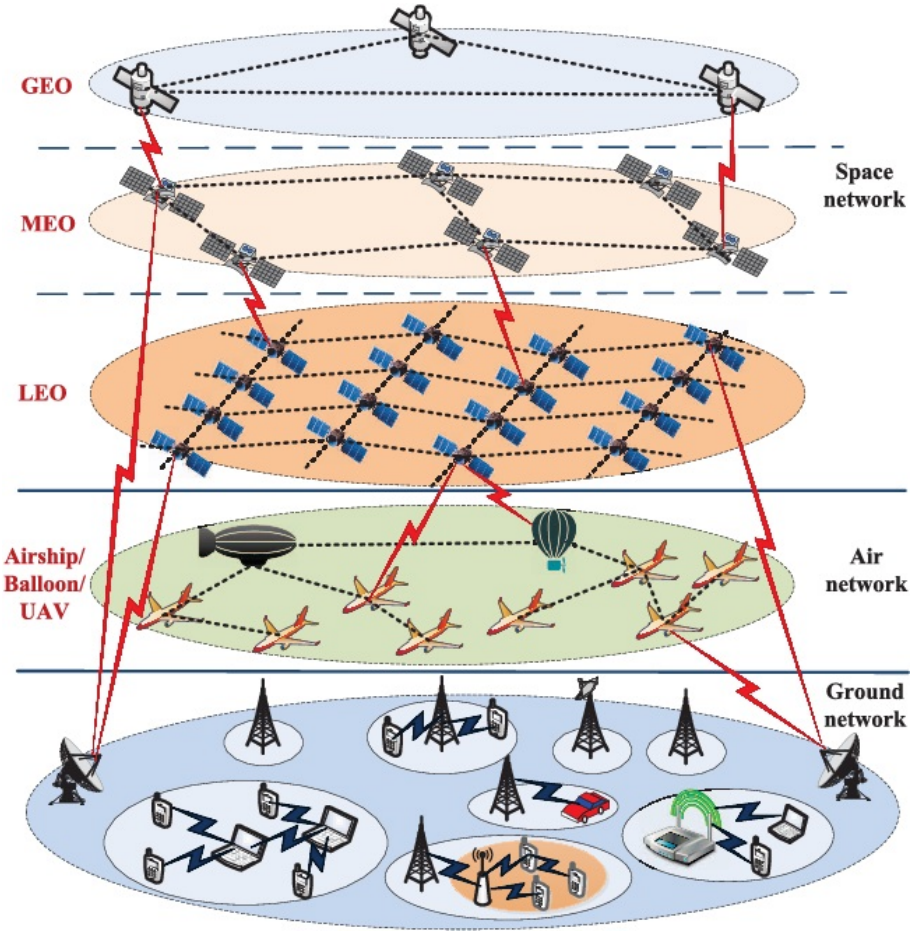


Figure 1.2 : Illustration of an Air-space-ground integrated information network [14].

- UAV-assisted communications. A UAV network can be used to assist other communications, such as the UAVs can be used as relays or aerial base stations to assist the terrestrial communication system and improve the network capacity and coverage. In addition, the UAV network can also be integrated with ground control stations, satellites, and other aircraft platforms, to form an integrated air-space-ground information network, as shown in Fig. 1.2. The mobility of the UAV systems can be exploited to achieve effective information relaying between different network layers. As an essential part of the air-space-ground integrated information network, the UAV network can effectively reduce the coverage holes.

1.2 Research Problems and Challenges

To accurately analyze the performance of the multi-UAV system (UAV network), we need to take into consideration some characteristics specific to UAV networks arise that differ from those other wireless networks, such as MANETs, VANETs, and traditional wireless sensor networks (WSNs).

The significant challenges or problems for UAV communication and networks are summarized as follows:

- **Challenge 1**: Aerial vehicles and their constraints. The vehicles used for aerial networking come in various forms due to the requirements of the applications they are deployed for [10]. The choice of vehicles affects the range of operation and the number of required vehicles. Large unmanned devices usually offer a longer range of connectivity over a single link since they can carry heavy dedicated transceivers, while small UAVs employing Wi-Fi compliant radios, the same range of connectivity can be expected using multiple devices with ad hoc networking.

- **Challenge 2**: Three-dimensional (3D) nature and radio propagation characteristics. The 3D nature of the network demands the support of various types of links. The links in an aerial network can be either air-air (A2A), air-ground (A2G) or ground-air (G2A). These links have been analyzed against each other as well as against ground-ground (G2G) links. The wireless channel is affected by elements in the 3D space, which corresponds to the terrain over which the UAV is flying, along with a number of obstacles in the space [10]. The 3D networks also have several accentuated concerns, such as variations in communication distance, direction of the communicating pairs, antenna radiation pattern, shadowing from the UAV, onboard electronic equipment, environmental conditions, interferences, and jamming [6]. The high mobility of the

devices in 3D space is also essential and needs to be considered, since antenna orientation, and hence link quality fluctuates widely with mobility [15].

- **Challenge 3**: High and random Mobility. Due to the high mobility of UAVs, the terrain over which the UAVs are flying is expected to change very frequently, for instance, from woodlands to lakes to buildings during a single flight. Not only do terrain-induced blind spots affect the wireless propagation channel, but they may also introduce frequent topology changes amongst multiple devices that require connectivity (UAVs, ground clients, and base stations). Besides, UAVs are characterized by the demand for mobility in 3D space. Therefore, not only may the terrain over which the UAVs are flying change frequently, but also the altitude of flight may have to be varied to avoid obstacles and collisions.

Security is also an essential consideration for the UAV-enabled wireless networks. On the one hand, the UAVs in the systems are susceptible to battery failures and device damage, which may lead to error and failure information transmission. Besides, these UAVs may store a wide range of information from troop movements to environmental data and strategic operations. The amount and kind of information enclosed make UAVs an extremely interesting target for espionage and endangers UAVs of theft, manipulation and attacks, such as malware attacks and localization attacks. External hostile nodes (unmanned nodes or ground nodes) may attempt to intercept information transmitted between legitimate UAVs or maliciously interfere with legitimate UAVs to affect their regular operation and communication. Therefore, it is necessary to research on the security architecture and technologies of the UAV-enabled wireless networks.

On the other hand, the multi-UAV system is also increasingly posing severe threats to information security and privacy. UAVs could be used as eavesdroppers

to sniff, intercept unauthorizedly, jam, and spoof wireless communications between legitimate terrestrial transceivers [16, 17]. The attractive merits of UAVs, such as excellent flexibility, maneuverability, mobility, and elevated positions, have the potential to increase security risks that UAVs can adversely pose [17]. It is of practical interest to understand the robustness of terrestrial wireless communications under exposure to new threats from aerial adversaries, such as aerial eavesdroppers [16].

1.3 Research Objectives and Contributions

1.3.1 Research Objectives

The aims of this thesis are to:

- **Objective 1:** analyze the link capacity of UAV pairs with random 3D trajectories in UAV-enabled wireless networks.
- **Objective 2:** analyze the coverage or connectivity of an uncoordinated UAV swarm, both in the absence and the presence of ground interference, where the UAVs fly with independent and random 3D flight trajectories.
- **Objective 3:** analyze the secure coverage or connectivity of a swarm of uncoordinated UAVs, both in the absence and the presence of ground interference, where the UAVs fly with independent and random 3D flight trajectories.
- **Objective 4:** investigate the threats that the aerial eavesdroppers can pose to terrestrial wireless communications. Establish the secrecy capacity for the ground transceivers in the case where the aerial eavesdroppers fly with random trajectories in a 3D spherical space.

1.3.2 Research Contributions

1. We propose a novel mathematical framework to analyze the link capacity of UAV communications, where UAVs have random 3D trajectories. The impact

of network densification, imperfect channel state information, and interference from ground transmitters on the link capacity is also captured. The analytical results provide new insight into the link capacity of UAV communications in 3D space and help compare diversity combining strategies in 3D fading channels.

2. We analyze the connectivity probability of any closest pair of individuals in a UAV swarm, where the aeronautic characteristics of UAVs, the changing topology of the UAV swarm in the 3D space, and ground interference are taken into account. As a result, asymptotically accurate closed-form expression is derived for the outage probability, which can specify the coverage region of the swarm with respect to the number of the UAVs, the transmit power, the Rician factor, and the outage probability constraint.

3. We propose an efficient hierarchical trust model (EHTM) that takes into consideration the UAVs' behaviors, the characteristics of channels between UAV nodes and the mobility of UAV nodes. The trustworthiness of the link between UAVs is quantified, and the impact of Doppler shift on the secure connectivity of the UAV networks is considered, based on the EHTM. The proposed trust model can effectively guarantee secure and reliable communication between UAVs and enhance the connectivity probability when the UAVNs suffer network attacks and other security risks.

4. We analyze the threat that aerial eavesdroppers can pose to terrestrial wireless communications from an information-theoretic point of view. The secrecy rate of the terrestrial link is analyzed. The impact of the collaboration of multiple aerial eavesdroppers using different diversity techniques is evaluated. The "cut-off" density of the eavesdroppers under which the secrecy rates vanish is identified to help specify the "no-flying" zone to protect important infrastruc-

tures.

1.4 Thesis Organization

This thesis focuses on the capacity and coverage analysis of the UAV-enabled wireless networks. The main research work and structure of this thesis are summarized as follows:

- *Chapter 1* As a brief introduction, Chapter 1 introduces the background, and discusses the challenges of UAV-enabled wireless networks.

- *Chapter 2* introduces the reference structure of UAV-enabled wireless networks and summarizes the related work on performance analysis of UAV-enabled wireless networks.

- *Chapter 3* analyzes the link capacity between autonomous UAVs with random 3D trajectories, and quantifies the impact of network densification on the capacity of the UAV networks.

- *Chapter 4* analyzes the connectivity of an uncoordinated UAV swarm, both in the absence and the presence of ground interference, and evaluates the reliability of the communication link in the uncoordinated UAV swarm.

- *Chapter 5* proposes a novel trust model that can evaluate the reliability and security of UAV-enabled wireless networks. The secure connectivity probability of the UAV pair in the presence of the Doppler shift is investigated.

- *Chapter 6* studies the threats that aerial eavesdroppers can pose to terrestrial wireless communications, from an information-theoretic point of view. The secrecy rate of the terrestrial link is analyzed for a ground transmitter-receiver pair, in the case where aerial eavesdroppers fly under random trajectories with smooth turns (STs) in 3D spherical space.

- *Chapter 7* concludes the analytical and simulation results discussed in earlier chapters of the thesis, and discusses the limitations and future research directions of this study.

Chapter 2

Literature Review

In this chapter, we review the related work on the UAV-enabled wireless networks, (secrecy) performance analysis of traditional wireless networks and UAV-enabled wireless networks.

2.1 UAV-enabled Wireless Network

In recent years, the application of UAVs has received extensive attention from research institutions and enterprises. Many projects have been launched, including UAV application in the fields of civil safety, disaster relief, monitoring, troubleshooting, entertainment, agriculture. In most public and civil applications, multi-UAV systems are configured to provide services collaboratively and extend the network coverage by acting as relays [6]. For instance, in [18, 19, 20], the concept of Aeronautical Ad Hoc Networks (AANET) was introduced, where the mobile routers were commercial aircraft, to alleviate the issue of resource scarcity. In AANET, an aircraft can initially download data from the Internet either directly from the ground or via satellite. The data can then be cached and shared with other aircraft in the proximity by dynamically establishing single or multi-hop paths to the requesting aircraft, using ad hoc networking principles. AANET system may be implemented and widely deployed much faster and with less investment due to the requirement of less infrastructure involved compared with satellite and ground station methods. Meshed ad hoc networking architectures were proposed in [21] to extend the operational envelope of small UAV, where UAVs in the network can self-organize to act as relays and forward data to the destination. Compared with other architectures,

the meshed communication architecture can offer better flexibility, reliability, and performance. Andre *et. al* [7] encouraged to exploit multi-hop WLAN to extend the operation coverage and the performance of the multiple UAV system.

2.2 Performance analysis of Wireless Networks

2.2.1 Performance analysis of Traditional wireless Networks

In a different yet relevant context of terrestrial wireless communications, a lot of studies have been conducted on analyzing the ergodic capacity, outage probability, and outage capacity in two-dimensional (2D) space. For example, Baccarelli and Fasano [22] derived the upper and lower bounds for the capacity of fading channels by exploiting the Jensen's inequality. A recurrence expression for the capacity of a Nakagami-m fading channel with binary phase shift keying (BPSK) modulation was developed in [23], with the assumption that channel state information (CSI) was available at the receiver. Rezki and Alouini [24] investigated the capacity of flat Rayleigh fading channels with ideal CSI at both the transmitter and receiver with asymptotically low signal-to-noise ratio (SNR) and established the scaling law of $\rho \log(1/\rho)$, where ρ is the SNR. In [25], the capacity of an $\alpha-\eta-\kappa-\mu$ fading channel was studied by using infinite series theory. In [26] and [27], the impact of MAC protocols on the capacity of vehicular networks was studied with a focus on the backoff timer designs of channel-sense multiple-access with collision avoidance (CSMA/CA). Hong *et.al.* [28] studied the statistics of the capacity of wide-band indoor channels, based on experimental measurements. All these works were based on 2D environment, and cannot incorporate 3D trajectories and mobility which are distinguishing features of UAVs.

Only a small number of studies have been carried out in 3D space. In [29], the achievable capacity of wireless social networks was derived as a function of the path loss exponent, the number of nodes, social group concentration, contact con-

centration, and the size of social group in the setting where nodes were uniformly distributed in a 3D cubic region. The link capacity and routing density were investigated in cognitive wireless networks with nodes uniformly distributed in a 3D cubic region in [30].

2.2.2 Performance analysis of UAV-enabled Wireless Networks

Little study has to date been carried out on the communication performance between autonomous UAVs with mobility consideration. Most existing studies have been on static settings of UAVs or simplified, deterministic trajectories. For instance, the ABSOLUTE project [31] adopted static or semi-static UAVs as aerial Long-Term Evolution Advanced (LTE-A) base stations (BSs) to provide wireless coverage during and after large-scale natural disasters. The UAVs were operated as unmanned aerial BSs and deployed as part of heterogeneous network architecture for public-safety communications [32, 33, 34]. The deployment of one or multiple stationary UAVs was shown to significantly enhance the network capacity and coverage [35, 36].

Under the stationary settings of UAVs, the expression of the outage probability in UAV networks was derived over Nakagami-m fading channels in [37]. Abualhaol and Matalgah in [38] analyzed the outage probability and the achievable bit rate of a cooperative multi-carrier UAV network over generalized Gaussian-Finite-Mixture fading channels. The analytical approximation, as well as simple upper and lower bounds of the ergodic capacity, were achieved in hybrid satellite-terrestrial relay networks [39]. In [40], aeronautical communication network was modeled as a mobile ad hoc network, and the throughput and average delay were analyzed. In [41], the total throughput and average delay under different scenarios or assumptions were analyzed for aeronautical communication networks. However, the impact of flight parameters and wireless channel parameters was also overlooked, as the constant link capacity was assumed implicitly. However, a constant link capacity was implicitly

assumed in these studies, and the impact of random flight trajectories and wireless channel parameters on the capacity and the connectivity of UAVs was typically overlooked or significantly simplified.

The outage probability of the downlink in a UAV network was derived over Nakagami-m fading channels in [37]. Abualhaol and Matalgah [38] analyzed the outage probability and the achievable bit rate of the downlink in a cooperative multi-carrier UAV network over generalized Gaussian-Finite-Mixture fading channels. The approximation, and the upper and lower bounds, of the ergodic capacity, were obtained in hybrid satellite-terrestrial relay networks in [39]. In [42], the coverage probability was derived for 3D UAV networks, where dynamic altitude control of interfering UAVs was modeled as random waypoint (RWP) mobility. In [36], the optimal 3D deployment of multiple UAVs was derived to maximize the downlink coverage of UAV-based communications over a given geographical area. Chetlur and Dhillon [43] studied the coverage performance for a UAV network where there were a number of UAVs with positions modeled as a uniform binomial point process (BPP) on a plane at a fixed altitude.

2.3 Physical Layer Security

2.3.1 Physical Layer Security in Traditional Wireless Networks

Physical layer security has been studied extensively in wireless fading channels. The secrecy performance, such as ergodic secrecy capacity, secrecy outage probability, or outage secrecy capacity, can be affected by channel fading and the positions of the transmitter, receiver, and eavesdropper. In [44], the secrecy outage probability and the probability of non-zero secrecy capacity for the Fisher-Snedecor $\mathcal{F}$ wiretap fading channel were analyzed in the presence of an active eavesdropper, and closed-form expressions were derived. Three new metrics for physical layer security over quasi-static fading channels were proposed in [45], including a generalized se-

crecy outage probability, asymptotic lower bound on eavesdropper's decoding error probability and average information leakage rate. The performance of fixed-rate wiretap codes was evaluated based on the metrics. In [46], the secrecy outage probability and the achievable average secrecy rate of the hybrid mmWave networks were analyzed by considering both the Nakagami-m fading and blockages. In [47], a closed-form expression for the secrecy outage probability of a wireless system including a BS, a legitimate user, and an eavesdropper, was derived as a function of the targeted transmission rate, where the eavesdropper's location was assumed to be randomly and uniformly distributed in a 2D ring-shaped area, centered at the BS. In [48], the secrecy performance of the Wyner's model was studied for vehicular-to-vehicular (V2V) communications in the presence of uncertainty in the eavesdropper's location. The above studies have been focused on 2D terrestrial wireless communications. Neither can they be extended to 3D space, nor incorporate specific 3D mobility models.

2.3.2 Physical Layer Security in UAV-enabled Wireless Networks

Only a small number of works have to date investigated the secrecy performance of UAV-enabled wireless networks. In [49, 50, 51, 52, 53], UAV-enabled wireless communication systems were studied, where UAVs were used as BSs or relays to improve the secrecy rate. In [49], the high mobility of a UAV was exploited to improve the secrecy rate of the UAV-to-ground (U2G) and ground-to-UAV (G2U) communications via joint trajectory and power control optimization. In [50], a new UAV-enabled mobile jamming scheme was developed to improve the secrecy rate of the ground wiretap channel. In [51], a UAV was deployed as a mobile relay to maximize the secrecy rate in a four-node system setup including a source, a mobile relay, a destination, and an eavesdropper. In [52, 53], two UAVs were employed, one for communications with ground nodes, and the other for jamming the

eavesdroppers on the ground. In [54], a downlink mmWave system was considered, where UAVs served as aerial BSs and sent data to a number of ground receivers in the presence of non-cooperative eavesdroppers on the ground. A Matérn Hardcore (MHC) spatial point process, which is an extension of the spatial Poisson point process with repulsion between points, was used to model the locations of the UAVs with minimum safety distances. The static ground eavesdroppers' locations followed a Poisson point process. The average secrecy rate of a UAV to a ground receiver was studied numerically. Liu et al. [55] analyzed the hybrid outage probability of UAV-aided wireless communications, by combining the transmission outage probability and the secrecy outage probability. In [56], the physical layer secrecy was studied for a U2G communication link with one or multiple potential eavesdroppers on the ground. The trajectory and transmit power of the UAV were jointly designed given a flight duration. In all these studies, UAVs have been used to assist terrestrial wireless communications, rather than being eavesdroppers. In [57], an aerial network was studied where relatively stationary aerial eavesdroppers were uniformly distributed within a 3D sphere centered at an aerial transmitter. Selection combining was carried out among the aerial eavesdroppers. The free-space channel model was assumed to analyze the secrecy outage probability and the average secrecy rate of the transmitter.

2.3.3 Performance Metrics for Physical Layer Security

The performance metrics that of interest are as follows.

2.3.3.1 Instantaneous secrecy capacity (bit/s/Hz)

The instantaneous secrecy capacity for one channel realization of the quasi-static fading channel between the ground transmitter and receiver can be given by [58]

$$\mathcal{C}^s = \begin{cases} \log_2(1+\zeta_r) - \log_2(1+\zeta_e), & \text{if } \zeta_r > \zeta_e; \\ 0, & \text{if } \zeta_r \leq \zeta_e, \end{cases} \tag{2.1}$$

where ζ_r is the instantaneous SNR at the legitimate receiver and ζ_e is the in the instantaneous SNR at the eavesdropper.

2.3.3.2 Ergodic secrecy capacity (bit/s/Hz)

The ergodic secrecy capacity is defined as the average secrecy rate of the channel between the ground transmitter and receiver, and represented as

$$\mathcal{C}^s_{\text{erg}} = \mathbb{E}\left[\mathcal{C}^s\right] = \begin{cases} \mathbb{E}\left[\log_2(1+\zeta_r) - \log_2(1+\zeta_e)\right], & \text{if } \zeta_r > \zeta_e; \\ 0, & \text{if } \zeta_r \leq \zeta_e. \end{cases} \tag{2.2}$$

2.3.3.3 Secrecy outage probability

The secrecy outage probability is defined as the probability that the instantaneous secrecy capacity is less than a target secrecy rate $\mathcal{R}_{\text{th}}$ ($\mathcal{R}_{\text{th}} > 0$), and given by

$$\begin{aligned} \mathcal{P}^s_{\text{out}} &= \Pr\left(\mathcal{C}^s < \mathcal{R}_{\text{th}}\right) \\ &= \Pr\left\{\log_2(1+\zeta_r) - \log_2(1+\zeta_e) < \mathcal{R}_{\text{th}}\right\}. \end{aligned} \tag{2.3}$$

2.3.3.4 ϵ-outage secrecy capacity

The outage secrecy capacity is defined as the maximum secrecy rate $\max\{\mathcal{R}_s\} = \mathcal{C}^s_{\text{out}}$ such that the outage probability is less than a certain value ϵ, that is, $\mathcal{P}^s_{\text{out}}\left[\mathcal{C}^s_{\text{out}}\right] = \epsilon$.

Chapter 3

Capacity Analysis of UAV-enabled Wireless Networks

3.1 Introduction

In this chapter, we analyze the link capacity between autonomous UAVs with random 3D trajectories. This is distinctively different from existing works typically under the assumption of either 2D or deterministic trajectories, and particularly interesting to applications such as surveillance and air combat.

A key contribution of this chapter is that we geometrically derive the probability distributions of the distances between a pair of UAVs which are assigned to serve the same 3D spaces but fly autonomously in an uncoordinated fashion. By exploiting the Jensen's inequality, the distributions are translated to the closed-form bounds for the ergodic capacity and outage capacity between the UAVs in 3D spaces. The analysis can also capture U2U links at fixed altitudes and U2G links between UAVs with 3D trajectories and static ground stations.

Another important contribution is that we extrapolate our analysis to dense 3D networks of UAVs, and quantify the impact of network densification on the capacity and coverage of the networks. By exploiting order statistics, the distances between adjacent UAVs are evaluated, and the closed-form lower bound for the multi-hop ergodic capacity is established.

Other contributions of this chapter also include the lower bounds for the ergodic capacity of U2U links in the presence of imperfect CSI at the receiver, and for the signal-to-interference-plus-noise ratio (SINR) in the presence of non-negligible

interference from ground transmitters. Validated by simulations, our analysis reveals that a U2U link with random 2D trajectories is superior in terms of outage capacity due to its short average link distance. It is also shown that a U2G link can incur substantially lower capacity than a U2U link, even in the case that the 3D coverage of the UAVs is the same. This results from the longer average length of U2G links.

The rest of this chapter is organized as follows. In Section 3.2, the system model and performance metrics are presented. In Section 3.3, the ergodic capacity and outage capacity of the U2U and U2G links are analyzed by evaluating the distributions of the link lengths. In Section 3.4, the analysis is extrapolated to study the impact of network densification on the capacity. In Section 3.5, the analyses are numerically validated by simulations, followed by the extensions of the analysis to the cases of imperfect CSI and non-negligible interference. In Section 3.7, conclusions are provided.

3.2 System Model and Problem Formulation

3.2.1 System Model

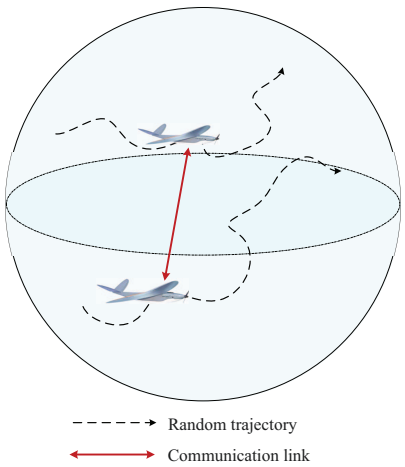


Figure 3.1 : Illustration on a pair of autonomous UAVs flying random 3D trajectories with smooth turns.

As illustrated in Fig. 3.1, the scenario that we consider involves two UAVs, each

equipped with an effective omni-directional antenna. To eliminate the body blockage resulting from the mobility and gesture changes of UAVs, the omni-directional antenna can be effectively implemented by deploying an array of antenna elements around the perimeter of a UAV, or attaching a pair of patch antennas on the upper and lower surfaces of the UAV. The different antenna elements, or patch antennas, can be aggregated at a radio frequency (RF) combiner/splitter before being connected to a single RF chain (including power amplifier, filter, up- and down-convertor, and analog-to-digital/digital-to-analogy convertor) and then a baseband digital signal processor, producing effectively a single omni-directional antenna free of body blockage.

The UAVs have independent 3D flight trajectories following a ST Mobility Model which incorporates centripetal and tangential accelerations and preserves the smoothness of aerial trajectories [59, 60]. The dynamics and constraints on the maneuverability of UAVs are captured. Moreover, the model has the important feature of uniform stationary distributions of UAV positions [60].

We also assume that there is no collision between the UAVs. The assumption is legitimate, provided the dimension of the UAVs is so small and negligible to the flight region. This is because of the continuous nature of the uniform node distributions, even in the case that the UAVs are uncoordinated and independently distributed, as dictated by the aforementioned property of the ST mobility model. The probability of UAV collisions approaches zero. In practice, collision-avoidance techniques are typically based on sensing and ranging. To broadcast safety messages can also prevent collisions. Our study on the channel capacity of UAVs can contribute to the prevention of collisions.

When one of the UAVs transmits to the other UAV, the received signal at the

latter is given by

$$y_r(t) = \sqrt{P} h_1 x(t) + n(t), \tag{3.1}$$

where P denotes the transmit power of the UAV, $x(t)$ is the transmit symbol*, and $n(t)$ is the zero-mean additive white Gaussian noise (AWGN) at the UAV with $\mathbb{E}\left[|n(t)|^2\right] = \sigma^2$. h_1 is the complex channel coefficient between the pair of UAVs, and it is assumed to be precisely known to the receiver unless otherwise specified.

The LoS links between UAVs are available in the open space. The U2U link is modeled to experience Rician fading, and the Rician factor K accounts for the influence of scattering and reflection from the surrounding environments. Particularly, K is defined to be the ratio between the signal power of the LoS path and the power of other scattered paths. We assume that the perfect CSI is available at the receiver. The probability density function (PDF) of the received SNR, denoted by ϑ, can be written as [61]

$$f_{\vartheta}(x) = \frac{1+K}{\bar{\vartheta}} \exp\left[-K - \frac{(1+K)x}{\bar{\vartheta}}\right] I_0\left(2\sqrt{\frac{K(K+1)}{\bar{\vartheta}}x}\right), \tag{3.2}$$

where $\bar{\vartheta} = \frac{P}{\sigma^2 l^{\alpha}}$ is the statistically average SNR; l is the distance between two UAVs; α is the large-scale path loss exponent; $I_0(x) = \sum_{n=0}^{\infty} \frac{(x/2)^{2n}}{n!\Gamma(n+1)}$ is the 0-th order modified Bessel function of the first kind; and $\Gamma(\cdot)$ is the gamma function.

3.2.2 Definitions of Performance Metrics

The performance metrics that we are particularly interested in are defined as follows.

*It is assumed that $x(t)$ follows a circularly symmetric complex Gaussian distribution $\mathcal{CN}(0,1)$, i.e., $\mathbb{E}[|x(t)|^2]$=1, where $\mathbb{E}[\cdot]$ denotes an expectation operation.

3.2.2.1 Ergodic capacity (bit/s/Hz).

This is a critical measure of the link between a pair of UAVs with random trajectories, and can be achieved by taking the average of the instantaneous capacity over all fading states. It is defined as [62]

$$C_{\text{erg}}\left(\vartheta\right)=\mathbb{E}\left[\log_2\left(1+\vartheta\right)\right]=\int_0^{\infty}\log_2\left(1+x\right)f_{\vartheta}\left(x\right)\,dx, \tag{3.3}$$

which, given the Rician fading channel, can be approximated to [62]

$$\begin{aligned} C_{\text{erg}}\left(\bar{\vartheta}\right) &\approx \frac{1}{\ln(2)}\left[\ln\left(1+\bar{\vartheta}\right)-\frac{\left(2K+1\right)\bar{\vartheta}^2}{2(1+K)^2\left(1+\bar{\vartheta}\right)^2}\right] \\ &= \frac{1}{\ln(2)}\left[\ln\left(1+\frac{P}{\sigma^2}l^{-\alpha}\right)-\frac{(2K+1)}{2(1+K)^2\left(1+\frac{\sigma^2}{P}l^{\alpha}\right)^2}\right] \\ &\triangleq C_{\text{erg1}}(l), \end{aligned} \tag{3.4}$$

given the statistically averaged SNR $\bar{\vartheta}=\frac{P}{\sigma^2 l^{\alpha}}$. The accuracy of this approximation was validated in [62, Fig. 1], and have been widely accepted and approved in the literature, e.g., [39].

We can prove that $C_{\text{erg1}}(l)$ is convex. This is because $\frac{d^2C_{\text{erg1}}(l)}{dl^2}\geq 0$ for $\alpha\leq\frac{1}{2}$ or $\alpha\geq\frac{121}{79}$, while the path loss exponent α is no less than 2 in practice. The detailed proof is provided in Appendix 3.8.1.

3.2.2.2 Outage Probability.

This metric defines the probability that the instantaneous SNR at the receiver is below a threshold ϑ_{th} required for successful reception [37, 38]. In the Rician fading

channel, it can be written as [61]

$$\begin{aligned} P_{\text{out}} &= \mathbb{P}\left(x \leq \vartheta_{th}\right) = \int_0^{\vartheta_{\text{th}}} f_{\vartheta}\left(x\right) dx \\ &= \int_0^{\vartheta_{\text{th}}} \frac{1+K}{\bar{\vartheta}} \exp\left(-K - \frac{1+K}{\bar{\vartheta}} x\right) I_0\left(2\sqrt{\frac{K\left(K+1\right)}{\bar{\vartheta}} x}\right) dx \\ &= 1 - Q\left(\sqrt{2K}, \sqrt{\frac{2\vartheta_{\text{th}}(1+K)}{\bar{\vartheta}}}\right), \end{aligned} \tag{3.5}$$

where $Q(\sqrt{a}, \sqrt{b}) = \int_b^{\infty} \frac{1}{2}\exp(-\frac{x+a}{2}) I_0(\sqrt{ax}) dx$ is the first-order Marcum Q-function. The SNR threshold ϑ_{th} is set up in prior, based on quality-of-service (QoS) requirements.

The first-order Marcum Q-function $Q(\sqrt{a}, \sqrt{b})$ can be approximated to [63]

$$\begin{aligned} & Q\left(\sqrt{2K}, \sqrt{\frac{2\vartheta_{\text{th}}(1+K)\sigma^2 l^{\alpha}}{P}}\right) \\ & \approx \exp\left[-e^{\nu\left(\sqrt{2K}\right)} \left(\frac{2\sigma^2 \vartheta_{\text{th}}(1+K) l^{\alpha}}{P}\right)^{\frac{1}{2}\mu\left(\sqrt{2K}\right)}\right] \triangleq \tilde{Q}\big(l\big) \end{aligned} \tag{3.6}$$

where $\nu\big(\sqrt{2K}\big)$ and $\mu\big(\sqrt{2K}\big)$ are non-negative parameters depending on K.

3.2.2.3 Outage Capacity (bit/s/Hz)

This metric defines the constant data rate which can be achieved with an outage probability less than the SNR threshold ϑ_{th}[64]. It can be written as

$$\begin{aligned} C_{\text{out}} &= \left(1 - P_{\text{out}}\right) \cdot \log_2\left(1 + \vartheta_{\text{th}}\right) \\ &= Q\left(\sqrt{2K}, \sqrt{\frac{2\vartheta_{\text{th}}(1+K)}{\bar{\vartheta}}}\right) \cdot \log_2(1 + \vartheta_{\text{th}}) \\ &\approx \tilde{Q}\big(l\big) \log_2(1 + \vartheta_{\text{th}}). \end{aligned} \tag{3.7}$$

Note that both the ergodic capacity and outage capacity provide the theoretical limits of practically achievable data rates. The ergodic capacity specifies the capacity

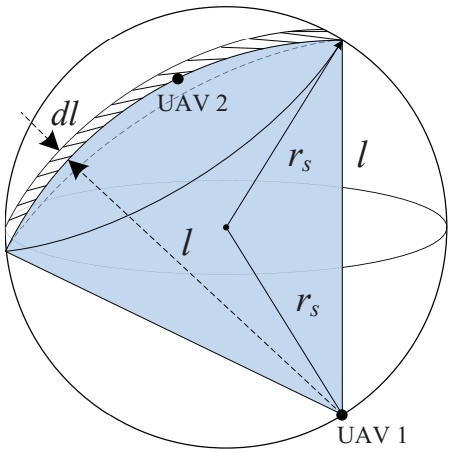


Figure 3.2 : Two UAVs in the spherical region (Special case: UAV 1 is located on the surface of the 3D spherical region).

of a channel, irrespective of the capability or operations of the transmitter and receiver (such as modulations). The outage capacity captures the capability of the receiver, and accounts for the receiver sensitivity ϑ_{th} which further depends on the modulation-and-coding schemes available to the transmitter-receiver pair. Moreover, recent advances on the coding theory are continuously closing the gap between the capacity and practically achievable data rate. For example, designs of Low-Density Parity-Check Codes were reported to achieve the channel capacity within 0.0045 dB of the Shannon Limit [65]. To this end, the analysis of the ergodic capacity and outage capacity is of practical value.

3.3 Link Capacity of UAV Communications

3.3.1 U2U Link with 3D Random Trajectories

We start with a general 3D scenario where two UAVs fly randomly in a 3D spherical region with radius r_s, as illustrated in Fig. 3.2. Given the uniform stationary distribution of each of the UAVs under the ST model, closed-form expressions for the ergodic capacity and outage capacity between the pair of UAVs can be evaluated.

A key step of our analysis is to evaluate the distance between the pair of UAVs

by exploiting the Crofton Fixed Point Theorem [66]. First, the Crofton Fixed Point Theorem is recalled in Lemma 1.

Lemma 1. *Suppose that N points ζ_i, $i = 1, 2, \cdots, N$, are randomly and independently distributed in a domain A with the volume $|A|$, and H depends on $\zeta_1, \cdots, \zeta_N$. Let $A' \subset A$, and δA is an infinitesimal boundary of A, but not in A'. Then the following relation holds:*

$$d\Pr\{H\} = N\left(\Pr\{H|\zeta_i \in \delta A\} - \Pr\{H\}\right)|A|^{-1}d|A|, \tag{3.8}$$

where $\Pr\{H|\zeta_i \in \delta A\}$ is the probability that H occurs when one of the random points ζ_i is on the boundary δA of A [66].

By exploiting the Crofton Fixed Point Theorem and the Jensen's inequality, we are able to establish the following theorem, namely, Theorem 1, on the ergodic capacity and outage capacity between the pair of UAVs flying random 3D trajectories with smooth turns.

Theorem 1. *For a pair of UAVs fly random trajectories with practical smooth turns in a 3D spherical region with the Rician fading, their ergodic capacity is lower bounded by*

$$C^*_{\text{erg1}} = \frac{1}{\ln(2)}\left[\ln\left(1+\frac{P}{\sigma^2}\left(\frac{36}{35}r_s\right)^{-\alpha}\right) - \frac{(2K+1)}{2(1+K)^2\left(1+\frac{\sigma^2}{P}\left(\frac{35}{36}r_s\right)^{\alpha}\right)^2}\right]; \tag{3.9}$$

and the outage capacity satisfies

$$\begin{cases} C_{\text{out1}} \geq C^*_{\text{out1}},\ \mathbb{E}[L_1] < l_{\text{th}} \\ C_{\text{out1}} \leq C^*_{\text{out1}},\ \mathbb{E}[L_1] \geq l_{\text{th}}, \end{cases} \tag{3.10}$$

where $l_{\text{th}} = \sqrt[\tau_3]{\frac{\tau_3 - 1}{\tau_1\tau_2\tau_3}}$, $\tau_1 = e^{\nu(\sqrt{2K})}$, $\tau_2 = \left(\frac{2\sigma^2\rho_{\text{th}}(1+K)}{P}\right)^{\frac{1}{2}\mu(\sqrt{2K})}$, $\tau_3 = \frac{1}{2}\alpha\mu\left(\sqrt{2K}\right)$,

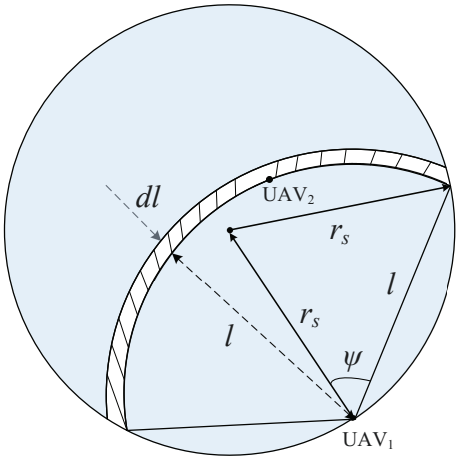


Figure 3.3 : Two UAVs in a 2D disk (Special case: UAV 1 is located on the boundary of the disk).

and

$$C^*_{\text{out1}} = \log_2(1+\vartheta_{\text{th}}) \exp\left[-e^{\nu\left(\sqrt{2K}\right)}\left(\frac{2\sigma^2\vartheta_{\text{th}}(1+K)\left(\frac{36}{35}r_s\right)^{\alpha}}{P}\right)^{\frac{1}{2}\mu\left(\sqrt{2K}\right)}\right]. \tag{3.11}$$

Proof. See Appendix 3.8.2. □

3.3.2 U2U Link with 2D Random Trajectories

The above analysis of random 3D trajectories with smooth turns is general, and can be extended to different interesting scenarios. One of the interesting scenarios is that two UAVs fly random 2D trajectories with smooth turns in a 2D sphere (or in other words, a disk) with radius r_s at a fixed altitude, as illustrated in Fig. 3.3. This 2D scenario is of interest to surveillance and monitoring applications. By extending Theorem 1, the following corollary can be obtained for the 2D scenario.

Corollary 1. *In the case that two UAVs fly random trajectories with smooth turns in a 2D spherical region with Rician fading, the lower bound for the ergodic capacity*

between the UAVs can be established as

$$C^*_{\text{erg2}} = \frac{1}{\ln(2)}\left[\ln\left(1+\frac{P}{\sigma^2}\left(\frac{128}{45\pi}r_s\right)^{-\alpha}\right) - \frac{(2K+1)}{2(1+K)^2\left(1+\frac{\sigma^2}{P}\left(\frac{45\pi}{128}r_s\right)^{\alpha}\right)^2}\right]. \quad (3.12)$$

and the outage capacity between the UAVs satisfies

$$\begin{cases} C_{\text{out2}} \geq C^*_{\text{out2}}, \text{ if } \mathbb{E}[L_2] < l_{\text{th}}; \\ C_{\text{out2}} \leq C^*_{\text{out2}}, \text{ if } \mathbb{E}[L_2] \geq l_{\text{th}}, \end{cases} \quad (3.13)$$

where

$$C^*_{\text{out2}} = \log_2(1+\vartheta_{\text{th}}) \exp\left[-e^{\nu\left(\sqrt{2K}\right)}\left(\frac{2\sigma^2\vartheta_{\text{th}}(1+K)\left(\frac{128}{45\pi}r_s\right)^{\alpha}}{P}\right)^{\frac{1}{2}\mu\left(\sqrt{2K}\right)}\right]. \quad (3.14)$$

Proof. See Appendix 3.8.3. □

3.3.3 U2G Link with 3D Random Trajectories

Another interesting scenario is that one UAV flies a random 3D trajectory with smooth turns, and communicates with a static ground station. This scenario can be analyzed by extending Theorem 1 as such that the ground station is fixed on the surface of the aforementioned 3D sphere while the UAV flies within the sphere.

Different from the analysis of a pair of UAVs, the altitude of the UAV can have a strong impact on the propagation characteristics of the U2G link, since the LoS path condition, and the environment between the UAV and the ground station, can alter as the elevation angle ϕ, $0 \leq \phi \leq \frac{\pi}{2}$. In other words, the Rician factor K can vary as a function of ϕ, i.e., $K = K(\phi)$. According to [67, 61], the Rician factor can be modeled as a non-increasing function of ϕ. A larger value of $\phi \in [0, \frac{\pi}{2}]$ leads to a higher LoS contribution and less multi-path scattering at the receiver, resulting in a larger Rician factor K. For the typically range of the Ricain factor K, $1 \leq K \leq 10$,

the Rician factor can be modeled as [61]:

$$K(\phi) = \kappa_0 \cdot \exp\left[\frac{2}{\pi} \ln\left(\frac{\kappa_{\frac{\pi}{2}}}{\kappa_0}\right) \phi\right], \tag{3.15}$$

where $\kappa_0 = K(0) = 1$ and $\kappa_{\frac{\pi}{2}} = K\left(\frac{\pi}{2}\right) = 10$ are environment- and frequency-dependent parameters.

Given the uniform stationary distribution of the UAV in the 3D sphere, the expectation of K can then be computed as:

$$\begin{aligned} \bar{K} = \mathbb{E}[K(\phi)] &= \int_0^{\frac{\pi}{2}} \phi\kappa_0 \exp\left[\frac{2}{\pi} \ln\left(\frac{\kappa_{\frac{\pi}{2}}}{\kappa_0}\right) \phi\right] d\phi \\ &= \frac{\pi^2 \kappa_{\frac{\pi}{2}}}{4 \ln\left(\frac{\kappa_{\frac{\pi}{2}}}{\kappa_0}\right)} \left[1 - \frac{1}{\ln\left(\frac{\kappa_{\frac{\pi}{2}}}{\kappa_0}\right)} + \frac{\kappa_0}{\kappa_{\frac{\pi}{2}} \ln\left(\frac{\kappa_{\frac{\pi}{2}}}{\kappa_0}\right)}\right]. \end{aligned} \tag{3.16}$$

By incorporating this elevation angle dependent Rician fading model into the analysis of Theorem 1, the following corollary can be established.

Corollary 2. *In the case that a UAV flies a random 3D trajectory with smooth turns in a Rician fading channel, the lower bound of the ergodic capacity between the UAV and a static ground station can be established as*

$$C^*_{\text{erg3}} = \frac{1}{\ln(2)} \left[\ln\left(1 + \frac{P}{\sigma^2}\left(\frac{6}{5} r_s\right)^{-\alpha}\right) - \frac{(2\bar{K}+1)}{2\left(1+\bar{K}\right)^2 \left(1 + \frac{\sigma^2}{P}\left(\frac{5}{6} r_s\right)^{\alpha}\right)^2}\right], \tag{3.17}$$

where $\bar{K} = \frac{\pi^2 \kappa_{\frac{\pi}{2}}}{4 \ln\left(\frac{\kappa_{\frac{\pi}{2}}}{\kappa_0}\right)} \left[1 - \frac{1}{\ln\left(\frac{\kappa_{\frac{\pi}{2}}}{\kappa_0}\right)} + \frac{\kappa_0}{\kappa_{\frac{\pi}{2}} \ln\left(\frac{\kappa_{\frac{\pi}{2}}}{\kappa_0}\right)}\right]$ *is the expectation of the Rician factor* K*,* $\kappa_0 = 1$ *and* $\kappa_{\frac{\pi}{2}} = 10$*.*

The outage capacity of the link satisfies

$$\begin{cases} C_{\text{out3}} \geq C^*_{\text{out3}}, \text{ if } \mathbb{E}[L_3] < l_{\text{th}}; \\ C_{\text{out3}} \leq C^*_{\text{out3}}, \text{ if } \mathbb{E}[L_3] \geq l_{\text{th}}, \end{cases} \tag{3.18}$$

where

$$C^*_{\text{out3}} = \log_2(1+\vartheta_{\text{th}}) \cdot \frac{2}{\pi} \int_0^{\frac{\pi}{2}} \exp\left[-e^{\nu\left(\sqrt{2K(\phi)}\right)} \times \left(\frac{2\sigma^2 \vartheta_{\text{th}} (1+K(\phi)) \left(\frac{6}{5} r_s\right)^{\alpha}}{P} \right)^{\frac{1}{2}\mu\left(\sqrt{2K(\phi)}\right)} \right] d\phi. \tag{3.19}$$

Proof. See Appendix 3.8.4. □

3.4 Network Densification and Relay

Another interesting extension of our analysis in Section 3.3 is to understand the impact of network densification on the capacity and coverage of UAVs with random 3D trajectories. Considering N UAVs with random 3D trajectories within the aforementioned 3D sphere, we are particularly interested in the case where the farthest two of the UAVs are the source and the destination, denoted by S and D, respectively; and the other UAVs act as relays, denoted by R_i, $i = 1, \cdots, N-2$.

3.4.1 Direct Link

Let l_{SD} denote the distance between the farthest pair of UAVs, i.e., S and D. l_{SD} is the longest of the distances between any pairs of the N UAVs in the 3D sphere. In the case that N is large, the cumulative distribution function (CDF) of l_{SD} can be given by [68, Theorem 1.1]

$$F_{l_{\text{SD}}}(x) = \Pr\{l_{\text{SD}} < x\} \to \exp\left\{ -\frac{3}{4}(2r_s - x)^3 N^2 \right\}. \tag{3.20}$$

The expectation of l_{SD} can be calculated as

$$\begin{aligned}\mathbb{E}\left[l_{\mathrm{SD}}\right] &\rightarrow \int_0^{2r_s} x\, dF_{l_{\mathrm{SD}}}(x) \\ &= \int_0^{2r_s} \frac{9}{4}N^2(2r_s-x)^2 x \exp\left[-\frac{3}{4}(2r_s-x)^3N^2\right] dx \\ &\overset{(a)}{=} \int_0^{2r_s} \frac{9}{4}(2r_s t^2 - t^3)N^2 \exp\left(-\frac{3}{4}N^2t^3\right) dt \\ &\overset{(b)}{=} \underbrace{\int_0^{2r_s} \frac{9}{2}N^2 r_s t^2 \exp\left(-\frac{3}{4}N^2t^3\right) dt}_{S_1} - \underbrace{\int_0^{2r_s} \frac{9}{4}N^2t^3 \exp\left(-\frac{3}{4}N^2t^3\right) dt}_{S_2},\end{aligned} \tag{3.21}$$

where (a) is obtained by setting $t = 2r_s - x$. S_1 and S_2 can be further given in closed-form by

$$S_1 = 2r_s\left[1 - \exp(-6N^2r_s^3)\right]; \tag{3.22}$$

$$\begin{aligned}S_2 &\overset{(c)}{=} \int_0^{6N^2r_s^3} (\frac{4}{3})^{\frac{1}{3}} N^{-\frac{2}{3}} v^{\frac{1}{3}} \exp(-v) dv \\ &\overset{(d)}{=} \sqrt[3]{\frac{4}{3}} N^{-\frac{2}{3}} \gamma\left(\frac{4}{3}, 6N^2r_s^3\right),\end{aligned} \tag{3.23}$$

where (c) is obtained by setting $v = \frac{3}{4}N^2t^3$; (d) is due to the identity integration $\int_0^u x^{\upsilon-1}\exp(-\varsigma x)dx = \varsigma^{-\upsilon}\gamma(\upsilon, \varsigma u)$ in [69, EH I 266(22), EH II 133(1)]; and $\gamma(a,b) = \int_0^b e^{-t}t^{a-1}dt$ is the incomplete gamma function.

Finally, we can rewrite (3.21) as

$$\mathbb{E}\left[l_{\mathrm{SD}}\right] = 2r_s\left[1 - \exp(-6N^2r_s^3)\right] - \sqrt[3]{\frac{4}{3}} N^{-\frac{2}{3}} \gamma\left(\frac{4}{3}, 6N^2r_s^3\right). \tag{3.24}$$

By exploiting the Jensen's inequality and the convexity of (3.4), the lower bound of the ergodic capacity of the farthest pair of UAVs, denoted by C^*_{erg4}, can be given by substituting (3.24) into (3.4).

3.4.2 Relayed Link

Let l_i, $i = 1, \cdots, N-1$, collect the Euclidean distances from an arbitrarily selected UAV to the other $(N-1)$ UAVs; and assume that l_i are independent and identically distributed (*i.i.d.*) random variables. Let $l_{\min}$ denote the shortest of the distances:

$$l_{\min} = \min_{i=1,\cdots,N-1} \{l_i\}. \tag{3.25}$$

Given (3.45), by exploiting order statistics, the CDF of $l_{\min}$ can be given by

$$\begin{aligned} F_{l_{\min}}(l) &= 1 - [1 - F_{L_1}(l)]^{N-1} \\ &= 1 - \left(1 - \frac{l^3}{r_s^3} + \frac{9l^4}{16r_s^4} - \frac{l^6}{32r_s^6}\right)^{N-1}, \end{aligned} \tag{3.26}$$

where $F_{L_1}(l) = \int_0^l f_{L_1}(l)dl$, and $F_{l_{\min}}(2r_s) = 1$.

As a result, the expectation of $l_{\min}$ can be given by

$$\begin{aligned} \mathbb{E}\left[l_{\min}\right] &= \int_{l=0}^{2r_s} l \; dF_{l_{\min}}(l) \\ &= -l\Big[-F_{L_1}(l)\Big]^{N-1}\Big|_0^{2r_s} + \int_0^{2r_s} \Big[1 - F_{L_1}(l)\Big]^{N-1} dl \\ &= \int_0^{2r_s} \left[1 - \frac{l^3}{r_s^3} + \frac{9l^4}{16r_s^4} - \frac{l^6}{32r_s^6}\right]^{N-1} dl. \end{aligned} \tag{3.27}$$

In the case that N is very large, i.e., $N \to \infty$, (3.27) can be rewritten as

$$\begin{aligned} \mathbb{E}\left[l_{\min}\right] &\approx \int_0^{r_s} \left(1 - \frac{l^3}{r_s^3}\right)^{N-1} dl + \int_{r_s}^{2r_s} \left(\frac{9l^4}{16r_s^4} - \frac{l^6}{32r_s^6}\right)^{N-1} dl \\ &= \frac{\Gamma(\frac{4}{3})\Gamma(N)}{\Gamma(N+\frac{1}{3})} r_s - \frac{3^{6N-5}}{2^{2N-\frac{3}{2}}} \left[\beta(\frac{1}{18}; 2N - \frac{3}{2}, N) - \beta(\frac{2}{9}; 2N - \frac{3}{2}, N)\right] r_s \\ &\approx \frac{\Gamma(\frac{4}{3})\Gamma(N)}{\Gamma(N+\frac{1}{3})} r_s, \end{aligned} \tag{3.28}$$

where the first approximation is taken since $1 - \frac{l^3}{r_s^3} > \frac{9l^4}{16r_s^4} - \frac{l^6}{32r_s^6}$ dominates the

integration over the region $[0, r_s)$ and $\frac{9l^4}{16r_s^4} - \frac{l^6}{32r_s^6} > 1 - \frac{l^3}{r_s^3}$ dominates over the region $(r_s, 2r_s]$, and $\beta(\cdot;\cdot,\cdot)$ stands for the generalized beta function.

Based on the Jensen's inequality and the convexity of (3.4), the lower bound of the average multi-hop ergodic capacity between the farthest pair of UAVs, denoted by C^*_{erg5}, can be given by substituting (3.28) into $\frac{1}{N-1}C_{\text{erg1}}(l)$, where $C_{\text{erg1}}(l)$ is given by (3.4) and $\frac{1}{N-1}$ is due to the worst-case propagation through all $(N-2)$ relays; or in other words, $(N-1)$ hops. Decode-and-Forward relay is assumed here, due to the consideration of the fast-changing topology of the UAVs; other relay strategies, such as amplify-and-forward, typically require stable topologies and are less relevant in this case.

3.5 Simulation and Evaluation

In this section, simulations are conducted to validate the analytical results presented in this chapter. The random trajectories of the UAVs are generated by using the ST mobility model [60]. The transmit power of UAVs, P, is set to be 20 dBm, unless otherwise specified. The noise power, σ^2, is set to be -80 dBm. Without loss of generality, we set the path loss exponent $\alpha = 3$, as assumed in [70, 71] for small UAV systems running data collection and ferrying in civil domains. It is important to note that our analysis is not restricted to a particular value of α, and can take other values for α. Other simulation parameters are listed in Tab. 3.1 with reference to [70, 71, 72].

Fig. 3.4 shows the ergodic capacity of the U2U links in both 2D and 3D spaces, and the U2G link in the 3D spaces, as the radii of the spherical regions, r_s, increase. Along with the analytical results dictated in Theorem 1, and Corollaries 1 and 2, Monte-Carlo simulation results are also plotted. We see that the analytical results coincide the simulation results, and provide tight lower bounds for the ergodic capacity. This confirms the validity of the proposed theorem and corollar-

Table 3.1 : Simulation parameters

Parameter	Value
Transmit power of UAV P	20 dBm
Noise power σ^2	-80 dBm
Path loss exponent α	3 [70, 71]
Rician factor K	0, 5, 10 dB
SNR threshold ϑ_{th}	0, 5, 10 dB

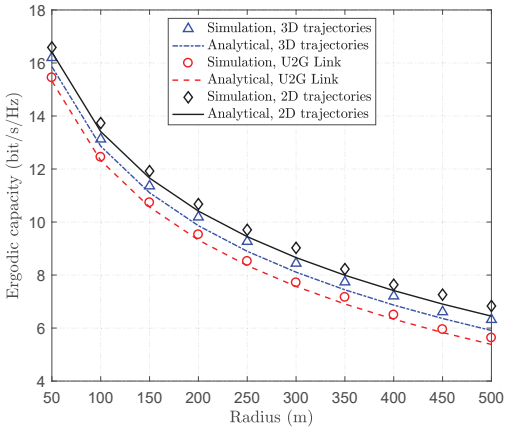


Figure 3.4 : The ergodic capacity vs. radius, with the Rician factor $K = 5$ dB, $P = 0.1$ W.

ies. As expected, we can see that the ergodic capacity declines with the radius. The decline slows down, as r_s grows. The ergodic capacity of each of the scenarios asymptotically converges to 0, as $r_s \to \infty$, as can be revealed in the theorem and corollaries.

In Fig. 3.4, we also see that the ergodic capacity of the U2U links is greater than that of the U2G link. One reason for this is because the U2G link suffers more scattering from the ground, resulting in larger fading. Another reason is that the average distance between the UAV and the fixed ground station, $\mathbb{E}[L_3] = \frac{6}{5} r_s$, is far longer than the distances between two UAVs with uncoordinated random trajectories, i.e., $\mathbb{E}[L_1] = \frac{36}{35} r_s$ in 3D spaces and $\mathbb{E}[L_2] = \frac{128}{45\pi} r_s$ in 2D spaces; see

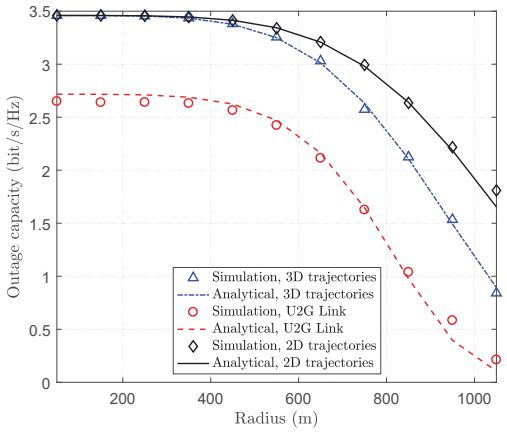


Figure 3.5 : The outage capacity vs. radius, with the Rician factor $K = 5$ dB, $P = 0.1$ W, and $\vartheta_{\text{th}} = 10$ dB.

Section 3.3.2. For the same reason, the U2U link with 2D random trajectories has a larger ergodic capacity than that with 3D random trajectories, since $\mathbb{E}[L_2] > \mathbb{E}[L_1]$.

Fig. 3.5 plots the outage capacity of the U2U links in both 2D and 3D spaces, and the U2G link in the 3D spaces, as the radii of the spherical regions, r_s, increase. By comparing the analytical results of Theorem 1, and Corollaries 1 and 2 with simulation results, the accuracy of the analysis is validated. We can see that the U2U link with 2D trajectories has the highest outage capacity, followed by the U2U link with 3D trajectories; and the outage capacity decreases, as the radius of the spherical regions grows. These are consistent with the results in Fig. 3.4. In Fig. 3.5, we also see that the gaps of the outage capacity increasingly enlarge between the three different settings of links. This is due to the fact that the outage capacity is defined to be the multiplicative product of the outage probability and ergodic capacity, both of which decrease with the growth of r_s. This multiplicative coupling effect can increasingly enlarge the differences between the link settings.

Fig. 3.6 plots the outage capacity of the U2U links in both the 2D and 3D spaces, and the U2G link in the 3D space against the SNR threshold ϑ_{th}, where the Rician factor $K = 5$ dB, $P = 0.1$ W and the radius of the spherical region $r_s = 500$

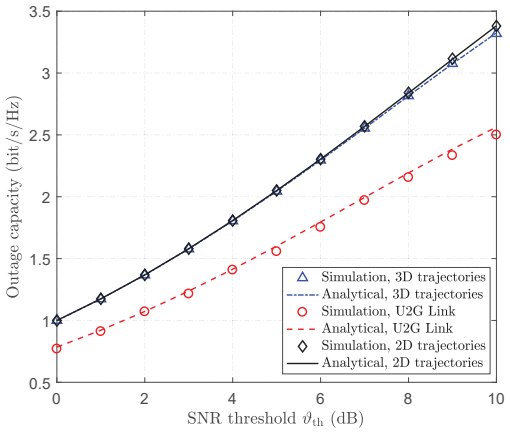


Figure 3.6 : The outage capacity vs. SNR threshold, with the Rician factor $K = 5$ dB, $P = 0.1$ W, and $r_s = 500$ m.

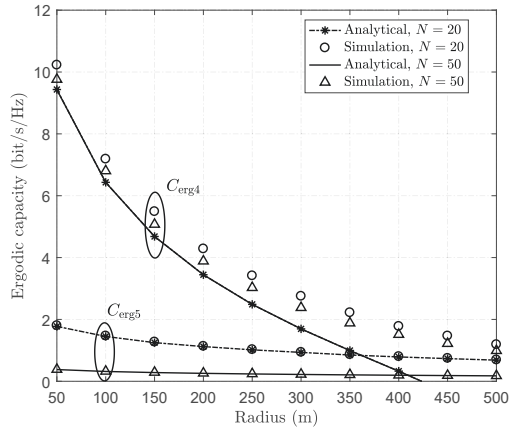


Figure 3.7 : The ergodic capacity vs. SNR threshold, with the Rician factor $K = 5$ dB, $P = 0.01$ W, and $\vartheta_{\text{th}} = 0$ dB.

m. We can see that the outage capacity of each of the link conditions increases almost linearly with the growth of ϑ_{th}. The difference between the U2U links with the 2D and 3D trajectories is marginal, especially for the low SNR thresholds. The difference between the U2U link and the U2G link is much larger, and increasingly enlarges with the growth of ϑ_{th}.

Last but not least, Fig. 3.7 evaluates the impact of network densification on the capacity and coverage of the UAVs with 3D trajectories, where the multi-hop ergodic

capacity and the direct ergodic capacity of the farthest pair of UAVs in the sphere, C_{erg5} and C_{erg4} , are plotted against the radius (or the coverage) of the sphere r_s. We can see C_{erg4} decreases rapidly with the growth of r_s. In contrast, the multi-hop ergodic capacity decreases slowly with the growth of r_s, and it also decreases with the growth of the number of UAVs N in the sphere. As an effective measure against network densification, the use of relay techniques can start to outperform the direct link when $r_s = 350$ m in the case of $N = 20$ and $r_s = 400$ m in the case of $N = 50$, as shown in the figure. We also see that the analytical results of the multi-hop ergodic capacity are fairly accurate, as an extension of Theorem 1 whose accuracy is validated in Fig. 3.4. However, the analytical results of the direct-link ergodic capacity is not tight. This is because the analysis is based on the assumption of $N \to \infty$, as discussed in Section 3.4.1.

3.6 Discussions and Extensions

3.6.1 Interference from the Ground Station

As reported in [61, 73], the aerial receivers are vulnerable to the interference coming from the ground transmitters. We proceed to discuss the impact of the interference from a fixed ground station on the link performance between a pair of UAVs flying random 3D trajectories with smooth turns.

The received signal at each of the UAVs can be written as

$$y = \sqrt{P} h_1 g_1 x(t) + \sqrt{P_I} h_I g_I x(t) + n(t), \tag{3.29}$$

where P_I is the transmit power of the ground transmitter, h_I is the channel fading coefficient between the ground transmitter and the UAV. $g_1 = {L_1}^{-\alpha}$ denotes the path loss between the UAVs with L_1 being the distance between two UAVs in the sphere. $g_I = {L_3}^{-\alpha_I}$ denotes the path loss between the designated UAV and the

ground station with α_I being the path loss exponent and L_3 being the distance between the UAV and the ground transmitter.

The SINR, denoted by Z, can be represented as

$$Z = \frac{PL_1{}^{-\alpha}|h_1|^2}{P_I L_3{}^{-\alpha_I}|h_I|^2 + \sigma^2} \triangleq \frac{X}{Y + \sigma^2}, \tag{3.30}$$

where $X \triangleq PL_1{}^{-\alpha}|h_1|^2$ and $Y \triangleq P_I L_3{}^{-\alpha_I}|h_I|^2$.

Since the channel h_1 follows the Rician distribution with parameter K and the channel h_I follows the Rician distribution with parameter K_I, the PDF of X can be written as

$$f_X(x) = \frac{1+K}{\Omega_x} \exp\left(-K - \frac{(1+K)x}{\Omega_x}\right) I_0\left(2\sqrt{\frac{K(1+K)}{\Omega_x}x}\right), \tag{3.31}$$

where $\Omega_x = PL_1{}^{-\alpha}$. Likewise, the PDF of Y can be given by replacing K, x and X with K_I, y and Y, respectively.

The expectation of X can be given by

$$\begin{aligned}
\bar{X} = \mathbb{E}[X] &= \int_0^\infty x f_X(x) dx \\
&= \frac{1+K}{\Omega_x} \exp(-K) \int_0^\infty x \exp\left(-\frac{(1+K)\,x}{\Omega_x}\right) \sum_{n=0}^{\infty} \frac{\left(\frac{K(1+K)x}{\Omega_x}\right)^n}{(n!)^2} dx \\
&= \frac{1+K}{\Omega_x} \exp(-K) \sum_{n=0}^{\infty} \frac{\left(\frac{K(1+K)}{\Omega_x}\right)^n}{(n!)^2} \int_0^\infty x^{n+1} \exp\left(-\frac{(1+K)x}{\Omega_x}\right) dx \\
&= \frac{\Omega_x}{1+K} \exp(-K) \sum_{n=0}^{\infty} \frac{K^n}{(n!)^2} \cdot (n+1)! \\
&= \frac{\Omega_x}{1+K} \exp(-K) \cdot (1+K) \exp(K) \\
&= \Omega_x = PL_1{}^{-\alpha}.
\end{aligned} \tag{3.32}$$

Similarly,

$$\begin{aligned}\bar{Y}' &= \mathbb{E}[Y+\sigma^2] = \mathbb{E}[Y]+\sigma^2 \\ &= \int_0^\infty y f_Y(y)dy + \sigma^2 \\ &= \Omega_y + \sigma^2 = P_I {L_3}^{-\alpha_I} + \sigma^2.\end{aligned} \tag{3.33}$$

The expectation of Z, denoted by $\bar{Z}$, can be obtained as

$$\begin{aligned}\bar{Z} = \mathbb{E}[Z] = \mathbb{E}\left[\frac{X}{Y+\sigma^2}\right] &\overset{(a)}{=} \mathbb{E}[X]\cdot\mathbb{E}\left[\frac{1}{Y+\sigma^2}\right] \\ &\overset{(b)}{\geq} \frac{\mathbb{E}[X]}{\mathbb{E}[Y+\sigma^2]} = \frac{P{L_1}^{-\alpha}}{P_I {L_3}^{-\alpha_I}+\sigma^2} \triangleq Z_1,\end{aligned} \tag{3.34}$$

where the equality (a) is due to the fact that X and Y are independent of each other. The inequality (b) is obtained from $\mathbb{E}\left[\frac{1}{Y+\sigma^2}\right] \geq \frac{1}{\mathbb{E}[Y+\sigma^2]}$ which is based on the Jensen's inequality (since $\frac{1}{Y+\sigma^2}$ is convex with respect to Y) [22].

From (3.34), we can find that $\frac{\partial^2 Z_1}{\partial L_1^2} \geq 0$ and $\frac{\partial^2 Z_1}{\partial L_3^2} \geq 0$. Z_1 is convex with respect to L_1 and L_3. By exploiting (3.46) and (3.58), the lower bound of $\mathbb{E}_{L_1,L_3}[Z_1]$ can be given by

$$\begin{aligned}\mathbb{E}_{L_1,L_3}[Z_1] &\geq \mathbb{E}_{L_3}[Z_1(\mathbb{E}[L_1])] \\ &\geq Z_1(\mathbb{E}[L_1],\mathbb{E}[L_3]) = \frac{P\left(\frac{36}{35}r_s\right)^{-\alpha}}{P_I\left(\frac{6}{5}r_s\right)^{-\alpha_I}+\sigma^2},\end{aligned} \tag{3.35}$$

where the inequality is based on the Jensen's inequality.

Fig. 3.8 plots both the analytical lower bound (3.35) and the simulation results for the SINR of a U2U link in the presence of the interference from a ground transmitter in a 3D space. The analytical results, i.e., SNR $= \frac{P}{\sigma^2}\left(\frac{36}{35}r_s\right)^{-\alpha}$, and the simulations of SNR of the U2U link (in the absence of the interference) are also plotted for reference. We can see that the analytical lower bounds of the SINR have marginal gaps from the simulation results of the SINR, and can becoming increasingly tight with the growth of the flying radius. We also see that the SINR can be significantly lower than the SNR, but can improve as the difference between the path loss exponents

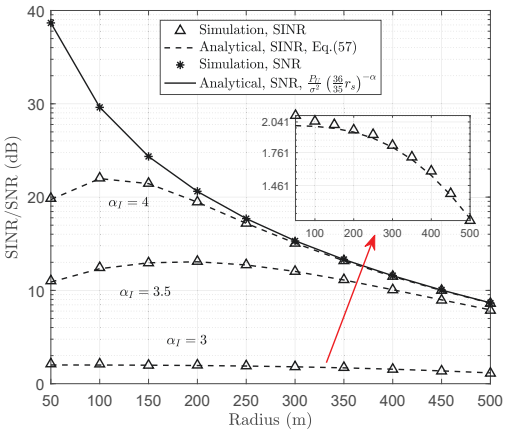


Figure 3.8 : SINR vs. radius, with $P = 0.1$ W, $P_I = 0.1$ W, and $\alpha = 3$.

α and α_I ($\alpha \geq \alpha_I$) increases. The conclusion drawn is that the interference from the ground transmitters can have strong impact on the performance of U2U links, especially in the case where the UAVs fly at low elevations, i.e., $\alpha_I \to \alpha$. It is important to mitigate the interference from the ground transmitters. A typical interference mitigation/avoidance technique is to use orthogonal time and frequency resources between UAVs and ground transmitters. Beamforming can also be carried out at the UAVs to nullify interferences in the spatial domain, provided that the UAVs are equipped with multiple antennas and can instantaneously estimate the channels from the ground transmitters [74]. Other possible techniques also include running listen-before-talk protocols at both the UAVs and ground transmitters, such as carrier-sense multiple access with collision avoidance (CSMA/CA) [26, 27]. This prevents nearby UAVs and/or ground transmitters from transmitting at the same time and the same frequency, hence avoiding intolerable interference.

3.6.2 Imperfect CSI at the Receiver

As discussed in [75, 76], the imperfect linear channel estimation based on a minimum mean-square error criterion can be performed and channel estimation errors occur. The imperfect CSI can be modelled as [77]: $h_1 = \hat{h}_1 + h_e$, where

$\hat{h}_1$ is the estimated CSI at the receiver, and h_e is a zero-mean, complex Gaussian estimation error which is independent of h_1 and has the variance ϵ. The received average SNR becomes

$$\bar{\vartheta}' = \frac{P{L_1}^{-\alpha}|\hat{h}_1|^2}{P{L_1}^{-\alpha}\epsilon + \sigma^2} = \frac{P|\hat{h}_1|^2}{P\epsilon + \sigma^2 {L_1}^{\alpha}}. \tag{3.36}$$

The ergodic capacity, C_{erg6}, can be written as

$$\begin{aligned} C_{\text{erg6}} &= C_{\text{erg1}}(\bar{\vartheta}') \\ &= \frac{1}{\ln(2)}\left[\ln\left(1+\frac{P}{P\epsilon+\sigma^2{L_1}^{\alpha}}\right) - \frac{(2K+1)}{2(1+K)^2\left(1+\epsilon+\frac{\sigma^2}{P}{L_1}^{\alpha}\right)^2}\right]. \end{aligned} \tag{3.37}$$

Given the convexity of $C_{\text{erg1}}(l)$, the lower bound of the ergodic capacity can be obtained by using the Jensen's inequality and (3.46), as given by

$$\begin{aligned} \mathbb{E}[C_{\text{erg6}}(L_1)] &\geq C_{\text{erg6}}(\mathbb{E}[L_1]) \\ &= \frac{1}{\ln(2)}\left[\ln\left(1+\frac{P}{P\epsilon+\sigma^2\left(\frac{36}{35}r_s\right)^{\alpha}}\right) - \frac{(2K+1)}{2(1+K)^2\left(1+\epsilon+\frac{\sigma^2}{P}\left(\frac{36}{35}r_s\right)^{\alpha}\right)^2}\right] \\ &\triangleq C^*_{\text{erg6}}. \end{aligned} \tag{3.38}$$

3.7 Conclusion

In this chapter, we analyzed the link capacity between autonomous UAVs with random 3D trajectories. Closed-form bounds for the capacity were derived between autonomous UAVs, and between UAVs and ground stations. The impact of network densification on the capacity, as well as the impacts of imperfect CSI and interference, were analyzed. Corroborated by simulations, our analysis showed that a U2U link with random 2D trajectories is superior that with random 3D trajectories in terms of capacity due to its short average link distance. It was also revealed that a

U2G link can incur substantially lower capacity than a U2U link even in the case that the 3D coverage of the UAVs is the same, as the result of longer average link length in the former case.

3.8 Appendix

3.8.1 Proof of the convexity of C_{erg1} with respect to l.

For notation simplicity, we let $\xi_1 = \frac{P}{\sigma^2}$ and $\xi_2 = \frac{2K+1}{2(1+K)^2}$, where $\xi_1 > 0$ and $\frac{21}{242} < \xi_2 < \frac{3}{8}$. C_{erg1} can be rewritten as

$$C_{\text{erg1}} = \frac{1}{\ln(2)} \left[\ln\left(1 + \xi_1 l^{-\alpha}\right) - \frac{\xi_2}{(1 + \frac{l^\alpha}{\xi_1})^2} \right]. \tag{3.39}$$

The first derivative of C_{erg1} with respect to l can be given by

$$\frac{dC_{\text{erg1}}(l)}{dl} = \frac{1}{\ln(2)} \left[\frac{-\xi_1 \alpha l^{-\alpha-1}}{1 + \xi_1 l^{-\alpha}} - \frac{\xi_2}{\xi_1} \cdot \frac{2\alpha l^{\alpha-1}}{(1 + \frac{l^\alpha}{\xi_1})^3} \right] \leq 0.$$

The second derivative of C_{erg1} can be given by

$$\begin{aligned}
\frac{d^2 C_{\text{erg1}}(l)}{dl^2} = \frac{1}{\ln(2)} \Bigg[& \frac{\xi_1(\alpha^2+\alpha) l^{-\alpha-2} + \xi_1^2 \alpha l^{-2\alpha-2}}{(1 + \xi_1 l^{-\alpha})^2} \\
& + \frac{\xi_2}{\xi_1^2} \cdot \frac{2\alpha(2\alpha-1) l^{2\alpha-2} - 2\xi_1 \alpha(\alpha-1) l^{\alpha-2}}{(1 + \frac{l^\alpha}{\xi_1})^4} \Bigg] \\
= \frac{1}{\ln(2)} \Bigg\{ & \underbrace{\left[\frac{\xi_1(\alpha^2+\alpha)}{(\xi_1 + l^\alpha)^2} - \frac{2\xi_2(2\alpha^2-\alpha)}{\xi_1(1 + \frac{l^\alpha}{\xi_1})^4} \right]}_{a(1)} l^{\alpha-2} \\
& + \underbrace{\left[\frac{\xi_1^2 \alpha}{(1 + \xi_1 l^{-\alpha})^2} l^{-2\alpha-2} + \frac{\xi_2 2\alpha(2\alpha-1)}{\xi_1^2 (1 + \frac{l^\alpha}{\xi_1})^4} l^{2\alpha-2} \right]}_{a(2) \geq 0} \Bigg\},
\end{aligned}$$

where

$$a(1) = \frac{\xi_1(\alpha^2+\alpha)}{(\xi_1+l^\alpha)^2} - \frac{2\xi_2\xi_1^3(2\alpha^2-\alpha)}{(\xi_1+l^\alpha)^4}$$
$$= \frac{\xi_1\left[(\alpha^2+\alpha)(\xi_1+l^\alpha)^2 + 2\xi_1^2\xi_2\alpha - 4\xi_1^2\xi_2\alpha^2)\right]}{(\xi_1+l^\alpha)^4}.$$

To achieve $a(1) \geq 0$, $(\alpha^2+\alpha-4\xi_2\alpha^2)\xi_1^2$ has to be larger than 0; or in other words, α must satisfy the following conditions: $\alpha \leq \frac{1}{2}$ or $\alpha \geq \frac{121}{79}$. Since α is the path loss exponent which is no less than 2 in nature, the second derivative of C_{erg1} is larger than 0, i.e., $\frac{d^2C_{\text{erg1}}(l)}{dl^2} \geq 0$. As a result, C_{erg1} is convex with respect to l.

3.8.2 Proof of Theorem 1.

We start by proving (3.9). To do this, we use L_1 to denote the Euclidean distance between the pair of UAVs, and $f_{L_1}(l)$ the PDF of L_1. We also let $\mathcal{P}$ denote the probability of two UAVs separated by distance l, and $\mathcal{P}_1$ denote this probability in the case that one of the UAVs is located on the surface of the sphere, as shown in Fig. 3.2.

According to the Crofton Fixed Point Theorem; see Lemma 1, we can have

$$d\mathcal{P} = 2\left(\mathcal{P}_1 - \mathcal{P}\right)|V|^{-1}d|V|, \tag{3.40}$$

where $|V|$ denotes the volume of the 3D sphere, i.e., $|V| = \frac{4}{3}\pi r_s^3$ and $d|V| = 4\pi r_s^2 dr_s$.

To evaluate $\mathcal{P}_1$, we set that UAV 1 is located on the surface of the sphere, then the other UAV, UAV 2, is located on the spherical cap centered at UAV 1 and with radius l in the sphere, as illustrated by the shaded part in Fig. 3.2. Let dl denote the thickness of the spherical cap. Therefore, the volume of the spherical cap is $2\pi l^2\left(1-\frac{l}{2r_s}\right)dl$. $\mathcal{P}_1$ can be obtained as

$$\mathcal{P}_1 = \frac{2\pi l^2\left(1-\frac{l}{2r_s}\right)dl}{\frac{4}{3}\pi r_s^3} = \frac{3l^2\left(2r_s-l\right)dl}{4r_s^4}. \tag{3.41}$$

Substituting (3.41) into (3.40), (3.40) can be rewritten as

$$d\mathcal{P} = 2\left(\frac{3l^2\left(2r_s - l\right)dl}{4r_s^4} - \mathcal{P}\right)\frac{3dr_s}{r_s}, \tag{3.42}$$

which, by mathematic manipulations, is further rewritten as

$$r_s^6 d\mathcal{P} + 6r_s^5\mathcal{P}dr_s = \left(9l^2r_s^2 - \frac{9}{2}l^3r_s\right)dldr_s. \tag{3.43}$$

Integrating both sides with respect to r_s, we obtain

$$\mathcal{P}r_s^6 = \int\left(9l^2r_s^2 - \frac{9}{2}l^3r_s\right)dldr_s = 9l^2dl\left(\frac{1}{3}r_s^3 - \frac{1}{4}lr_s^2\right) + c_1, \tag{3.44}$$

where c_1 is a constant to be determined.

We note that in the case $r_s = \frac{l}{2}$, both UAVs are uniquely located at the two ends of a diameter, and both on the surface of the sphere. Given the continuous nature of $\mathcal{P}$, the probability of $r_s = \frac{l}{2}$ is 0, i.e., $\mathcal{P} = 0$. By substituting this into (3.44), $c_1 = \frac{3}{16}l^5dl$, and the PDF of l can be given by

$$f_{L_1}(l) = \frac{3l^2}{r_s^3} - \frac{9l^3}{4r_s^4} + \frac{3l^5}{16r_s^6},\ 0 \le l \le 2r_s, \tag{3.45}$$

The average distance between the UAVs can be obtained as

$$\mathbb{E}[L_1] = \int_0^{2r_s} l \cdot f_{L_1}(l)\ dl = \frac{36}{35}r_s. \tag{3.46}$$

Based on the Jensen's inequality and the aforementioned convexity of $C_{\text{erg1}}(l)$, as discussed in Section 3.2.2.1, the lower bound of the ergodic capacity can be

established as

$$\begin{aligned}\mathbb{E}\Big[C_{\text{erg1}}(l)\Big] &\geq C_{\text{erg1}}\left(\mathbb{E}[L_1]\right)\\ &= \frac{1}{\ln(2)}\left[\ln\left(1+\frac{P}{\sigma^2}\left(\frac{36}{35}r_s\right)^{-\alpha}\right)-\frac{(2K+1)}{2(1+K)^2\left(1+\frac{\sigma^2}{P}\left(\frac{35}{36}r_s\right)^{\alpha}\right)^2}\right]\\ &\triangleq C^*_{\text{erg1}}.\end{aligned} \tag{3.47}$$

This concludes the proof of (3.9).

We proceed to prove (3.10). To do this, it is important to first evaluate the convexity and concavity of $\tilde{Q}(l)$. According to [63], the values of $\nu\big(\sqrt{2K}\big)$ and $\mu\big(\sqrt{2K}\big)$ in (4.2) can be obtained for the Rician factor of interest, i.e., $1 \leq K \leq 10$:

1. In the case of $1 \leq K \leq 10$, $\nu\big(\sqrt{2K}\big)$ and $\mu\big(\sqrt{2K}\big)$ are given by [63]

$$\begin{aligned}\mu\big(\sqrt{2K}\big) =& 2.174 - 0.592\sqrt{2K} + 0.593\big(\sqrt{2K}\big)^2\\ &- 0.092\big(\sqrt{2K}\big)^3 + 0.005\big(\sqrt{2K}\big)^4,\end{aligned} \tag{3.48}$$

$$\begin{aligned}\nu\big(\sqrt{2K}\big) =& -0.840 + 0.372\sqrt{2K} - 0.74\big(\sqrt{2K}\big)^2\\ &+ 0.083\big(\sqrt{2K}\big)^3 - 0.004\big(\sqrt{2K}\big)^4.\end{aligned} \tag{3.49}$$

2. In the case of $K = 0$, $\mu_0 = 2$ and $\nu_0 = -\ln 2$.

In both cases, we have $\nu\big(\sqrt{2K}\big) < -1$ and $\mu\big(\sqrt{2K}\big) \geq 2$. The convexity and concavity of $\tilde{Q}(l)$ can be judiciously evaluated. This is critical to the development of the bounds of the outage capacity with the use of the Jensen's inequality. To evaluate the convexity and concavity of $\tilde{Q}(l)$, the second-order derivative of $\tilde{Q}(l)$ is given by

$$\frac{d^2\tilde{Q}(l)}{dl^2} = \Big[(\tau_1\tau_2\tau_3)^2 l^{2\tau_3-2} - \tau_1\tau_2\tau_3(\tau_3-1)l^{\tau_3-2}\Big]e^{-\tau_1\tau_2 l^{\tau_3}}, \tag{3.50}$$

where, for notation simplicity, $\tau_1 = e^{\nu(\sqrt{2K})}$, $\tau_2 = \left(\frac{2\sigma^2\vartheta_{\text{th}}(1+K)}{P}\right)^{\frac{1}{2}\mu(\sqrt{2K})}$, and $\tau_3 =$

$\frac{1}{2}\alpha\mu\left(\sqrt{2K}\right)$.

Clearly, the sign of $\frac{d^2\tilde{Q}(l)}{dl^2}$ solely depends on $\left[(\tau_1\tau_2\tau_3)^2 l^{2\tau_3-2} - \tau_1\tau_2\tau_3(\tau_3-1)l^{\tau_3-2}\right]$. In the case that $l < \sqrt[\tau_3]{\frac{\tau_3-1}{\tau_1\tau_2\tau_3}} \triangleq l_{\text{th}}$, $\frac{d^2\tilde{Q}(l)}{dl^2} < 0$ and $\tilde{Q}(l)$ is concave with respect to l. Therefore, if $\mathbb{E}[L_1] < l_{\text{th}}$, the upper bound for the expectation of the outage capacity, denoted by $\mathbb{E}\big[C_{\text{out1}}\big]$, can be obtained by taking the expectation of (3.7), as given by

$$\begin{aligned}
\mathbb{E}\big[C_{\text{out1}}\big] &\approx \mathbb{E}\big[\tilde{Q}(l)\big] \cdot \log_2(1+\vartheta_{\text{th}}) \\
&\leq \tilde{Q}\left(\mathbb{E}[L_1]\right) \cdot \log_2(1+\vartheta_{\text{th}}) \\
&= \log_2(1+\vartheta_{\text{th}}) \exp\left[-e^{\nu\left(\sqrt{2K}\right)}\left(\frac{2\sigma^2\vartheta_{\text{th}}(1+K)\left(\frac{36}{35}r_s\right)^{\alpha}}{P}\right)^{\frac{1}{2}\mu\left(\sqrt{2K}\right)}\right] \\
&\triangleq C^*_{\text{out1}}, \text{ if } \mathbb{E}[L_1] < l_{\text{th}},
\end{aligned} \tag{3.51}$$

where the inequality is due to the exploitation of the Jensen's inequality and and the concavity of $\tilde{Q}(l)$, and the last equality is achieved by first plugging (4.2) and then substituting $\mathbb{E}[L_1] = \frac{36}{35}r_s$ from (3.46).

In the case that $l \geq l_{\text{th}}$, $\frac{d^2\tilde{Q}(l)}{dl^2} \geq 0$ and $\tilde{Q}(l)$ is convex with respect to l. Therefore, if $\mathbb{E}[L_1] \geq l_{\text{th}}$, the upper bound for $\mathbb{E}\big[C_{\text{out1}}\big]$ can be obtained as

$$\mathbb{E}\big[C_{\text{out1}}\big] \geq C^*_{\text{out1}}, \text{ if } \mathbb{E}[L_1] \geq l_{\text{th}}. \tag{3.52}$$

This concludes the proof of (3.10).

3.8.3 Proof of Corollary 1.

Let L_2 denote the distance between the pair of UAVs. With reference to (3.40), the PDF of L_2, denoted by $f_{L_2}(l)$, can be obtained by exploiting the Crofton fixed points theorem. Let $\mathcal{P}'$ denote the probability that the two UAVs are separated by the distance l, and $\mathcal{P}_2$ denote the same probability that one of the UAVs is on the

boundary of the disk. By referring to (3.40), we can obtain

$$d\mathcal{P}' = 2(\mathcal{P}_2 - \mathcal{P}')|S|^{-1}d|S|, \tag{3.53}$$

where $|S|$ is the area of the disk, i.e., $|S| = \pi {r_s}^2$ and $d|S| = 2\pi r_s dr_s$. UAV 1 is located on the boundary of the disk, and UAV 2 is located on the part of an arch centered at UAV 1, with radius l, and inside the disk, as illustrated by the shaded part in Fig. 3.3. We use dl to denote the thickness of the arch. The area of the arch is $2\psi l dl$. $\mathcal{P}_2$ can be obtained as

$$\mathcal{P}_2 = \frac{2ldl \arccos\left(\frac{l}{2r_s}\right)}{\pi {r_s}^2}. \tag{3.54}$$

By referring to the evaluation of $f_{L_1}(l)$, the PDF of L_2 can be given by

$$f_{L_2}(l) = \frac{2l}{{r_s}^2}\left(\frac{2}{\pi}\cos^{-1}\left(\frac{l}{2r_s}\right) - \frac{l}{\pi r_s}\sqrt{1-\frac{l^2}{4{r_s}^2}}\right), \text{ if } 0 \le l \le 2r_s. \tag{3.55}$$

From (3.55), the expectation of L_3 can be evaluated by

$$\begin{aligned}
\mathbb{E}[L_2] &= \int_0^{2r_s} l \cdot f_{L_2}(l) dl \\
&= \int_0^{2r_s} \frac{2l^2}{{r_s}^2}\left(\frac{2}{\pi}\cos^{-1}\left(\frac{l}{2r_s}\right) - \frac{l}{\pi r_s}\sqrt{1-\frac{l^2}{4{r_s}^2}}\right) dl \\
&= \frac{128}{45\pi} r_s.
\end{aligned} \tag{3.56}$$

Given $\mathbb{E}[L_2]$, the rest of this proof can follow the proof of Theorem 1, and therefore be suppressed here.

3.8.4 Proof of Corollary 2.

Let L_3 denote the distance between the UAV and the ground station. Based on (3.41), we can obtain the PDF of the distance L_3, as given by

$$f_{L_3}(l) = \frac{\mathcal{P}_1}{dl} = \frac{3l^2\left(2r_s - l\right)}{4r_s^4},\ 0 \le l \le 2r_s. \tag{3.57}$$

The expectation of L_3 is given by

$$\mathbb{E}(L_3) = \int_0^{2r_s} l f_{L_3}(l) dl = \int_0^{2r_s} \left(\frac{3l^3}{2r_s^3} - \frac{3l^4}{4r_s^4}\right) dl = \frac{6}{5} r_s. \tag{3.58}$$

With reference to the proof of Theorem 1, the lower bound of C_{erg3} is can be obtained as

$$\begin{aligned}
\mathbb{E}_{K,L_3}\left[C_{\text{erg1}}\right] &\ge \mathbb{E}_{L_3}[C_{\text{erg1}}\left[\mathbb{E}(K)\right]] \\
&\ge C_{\text{erg1}}\left[\mathbb{E}(K), \mathbb{E}(L_3)\right] \\
&= \frac{1}{\ln(2)}\left[\ln\left(1 + \frac{P}{\sigma^2}\left(\frac{6}{5}r_s\right)^{-\alpha}\right) - \frac{(2\bar{K}+1)}{2\left(1+\bar{K}\right)^2\left(1+\frac{\sigma^2}{P}\left(\frac{5}{6}r_s\right)^{\alpha}\right)^2}\right] \\
&= C^*_{\text{erg3}},
\end{aligned} \tag{3.59}$$

where $\mathbb{E}_{K,L_3}[\cdot]$ takes expectation over K and L_3.

In the case that $\mathbb{E}[L_3] < l_{\text{th}}$, the lower bound for the expectation of the outage capacity, denoted by $\mathbb{E}\big[C_{\text{out3}}\big]$, can be obtained by referring to (3.51), as given by

$$\begin{aligned}
\mathbb{E}_{K,L_3}\big[C_{\text{out3}}\big] &\le \mathbb{E}_K[\tilde{Q}_1\left(\mathbb{E}[L_3]\right)] \cdot \log_2(1+\vartheta_{\text{th}}) \\
&= \log_2(1+\vartheta_{\text{th}})\frac{2}{\pi}\int_0^{\frac{\pi}{2}} \exp\left[-e^{\nu\left(\sqrt{2K(\phi)}\right)}\right. \\
&\quad \left.\times\left(\frac{2\sigma^2\vartheta_{\text{th}}(1+K(\phi))\left(\frac{6}{5}r_s\right)^{\alpha}}{P}\right)^{\frac{1}{2}\mu\left(\sqrt{2K(\phi)}\right)}\right] d\phi \\
&\triangleq C^*_{\text{out3}},\ \text{if } \mathbb{E}[L_3] < l_{\text{th}}.
\end{aligned} \tag{3.60}$$

In the case that $\mathbb{E}[L_3] \geq l_{\text{th}}$, the upper bound for $\mathbb{E}\big[C_{\text{out3}}\big]$ can be obtained as

$$\mathbb{E}\big[C_{\text{out3}}\big] \geq C^*_{\text{out3}}, \text{ if } \mathbb{E}[L_3] \geq l_{\text{th}}. \tag{3.61}$$

This concludes the proof of Corollary 2.

Chapter 4

Connectivity Analysis of UAV-enabled Wireless Networks

4.1 Introduction

In this chapter, we analyze the connectivity of an uncoordinated UAV swarm, where each UAV flies autonomously along an independent and random trajectory with practical smooth turns in 3D spaces. Rician channel fading is considered to capture the body blockage and reflections of the UAVs. Non-negligible ground interference is taken into account. Our analysis involves deriving the stationary 3D distributions of UAVs by exploiting Crofton Fixed Point Theorem. Our analysis also involves approximations of Rician channel capacity by using the first-order Marcum Q-function to quantify the instantaneous outage probability of a UAV. The approximation in coupling with the Jensen's inequality can deliver closed-form bounds for the average one-hop outage probability and broadcast outage probability of the UAV. The qualifying condition of the bounds in terms of UAV coverage, l_{th}, is identified. By comparing the outage probabilities in the absence and the presence of ground interferences, we are also able to quantify the impact of the ground interference on the outage of the UAVs. Our analytical results are validated by extensive simulations and serve as firm bounds for the connectivities of a dense uncoordinated UAV swarm in 3D space. The analysis also provides insights and theoretical limits for trajectory planning, and others practical value to many applications, such as goods delivery and air combat. While motivated by UAV swarms, our analysis is general and can be applied to terrestrial networks.

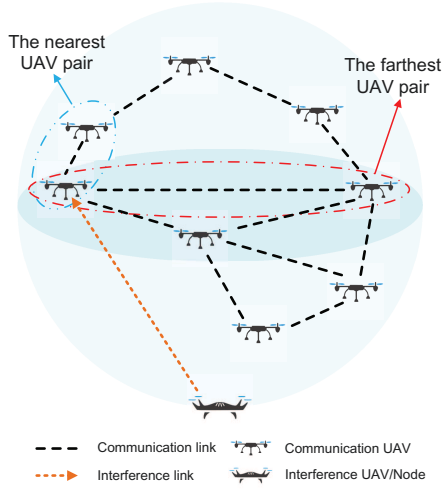


Figure 4.1 : A UAV swarm flies autonomously and randomly within a 3D sphere.

The rest of this chapter is organized as follows. In Section 4.2, the system model is described. In Section 4.3 and 4.4, we analyze the connectivity of individual UAVs, as well as the broadcast connectivity of the UAV swarm, in the absence and presence of the interference from the ground transmitters, respectively. In Section 4.5, simulation results are presented to validate the accuracy of our analytical results, followed by concluding remarks in Section 4.6.

4.2 System Model and Problem Formulation

In this section, the system structure of a UAV swarm, the channel model, and the mobility model of individual UAVs are described.

We consider a swarm of N UAVs flying autonomously within a 3D sphere, denoted by V, with radius r and volume $|V|$, as illustrated in Fig. 4.1. The radius of the sphere indicates the coverage of the UAV swarm. For illustration convenience, we assume that each UAV is equipped with a single antenna. CSMA/CA or TDMA can be adopted by the UAVs to share the same radio channel. Once the channel is occupied by a UAV, no others would transmit and produce interferences.

We start with an interference-free scenario, where the UAV swarm is far away

from any ground transmitters. (In Section 4.4, we will study a more general scenario where there can be interferences from a ground transmitters.) Let $s(t)$ denote the radio signal that UAV A transmits to UAV B. The received signal at UAV B is given by

$$y(t) = \sqrt{P}h(t)s(t) + n(t),$$

where $s(t)$ follows a circularly symmetric complex Gaussian distribution $\mathcal{CN}(0,1)$, i.e., $\mathbb{E}\left[\,|s(t)|^2\,\right] = 1$, $|\cdot|$ denotes norm, and $\mathbb{E}[\cdot]$ denotes expectation; P is the transmit power of each UAV; $h(t)$ is the channel coefficient between the pair of UAVs; and $n(t)$ is the AWGN with $\mathbb{E}\left[|n(t)|^2\right] = \sigma^2$.

LoS prevails in open spaces. Therefore, we model a UAV-to-UAV channel as an *i.i.d.* Rician fading channel. The PDF of the received SNR, denoted as x, is given by [61]

$$f_\rho(x) = \frac{1+K}{\bar{\rho}} \exp\left(-K - \frac{(1+K)x}{\bar{\rho}}\right) I_0\left(\sqrt{\frac{K(K+1)}{\bar{\rho}}x}\right),$$

where K is the Rician factor and indicates the ratio between the power in the direct path and the scattered paths, $0 \leq K \leq 10$; $\bar{\rho} = \frac{P}{\sigma^2 l^\alpha}$ is the average SNR of the link; l is the distance between the pair of UAVs; α is the large-scale path loss exponent; $I_0(x) = \sum_{n=0}^{\infty} \frac{(x/2)^{2n}}{n!\Gamma(n+1)}$ is the zero-th order modified Bessel function of the first kind [69]; and $\Gamma(z) = \int_0^\infty \frac{t^{z-1}}{e^t} dt$ is the Gamma function.

4.2.1 Outage Probability

The outage probability defines the probability that the received SNR is below a threshold ρ_{th} that is necessary for successful reception [37, 38]. Given the *i.i.d.*

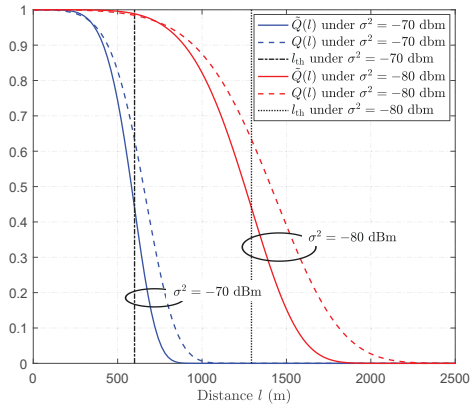


Figure 4.2 : The curve of $\tilde{Q}(l)$ vs. distance l, where $K = 5$ dB, $\rho_{\rm th} = 5$ dB, $P = 0.1$ W and $\sigma^2 = -70, -80$ dBm.

Rician fading between any pair of UAVs, the outage probability can be written as

$$\begin{aligned} P_{\rm out} &= \Pr\left(\frac{P|h(t)|^2}{\sigma^2 l^\alpha} \le \rho_{\rm th}\right) \\ &= \int_0^{\rho_{\rm th}} \frac{1+K}{\bar{\rho}} \exp\left(-K - \frac{1+K}{\bar{\rho}}x\right) I_0\left(2\sqrt{\frac{K\,(K+1)}{\bar{\rho}}x}\right)dx \\ &= 1 - Q\left(\sqrt{2K}, \sqrt{\frac{2\rho_{\rm th}(1+K)\sigma^2 l^\alpha}{P}}\right), \end{aligned} \tag{4.1}$$

where $Q(\sqrt{a}, \sqrt{b}) = \int_b^\infty \frac{1}{2}\exp(-\frac{x+a}{2})I_0(\sqrt{ax})dx$ is the first-order Marcum Q-function [61, Eq. 8].

The first-order Marcum Q-function $Q(\sqrt{a}, \sqrt{b})$ can be approximated to [63]:

$$Q\left(\sqrt{2K}, \sqrt{\frac{2\rho_{\rm th}(1+K)\sigma^2 l^\alpha}{P}}\right) \approx \exp\left[-e^{\nu(\sqrt{2K})}\left(\frac{2\sigma^2\rho_{\rm th}(1+K)l^\alpha}{P}\right)^{\frac{1}{2}\mu\left(\sqrt{2K}\right)}\right] \triangleq \tilde{Q}(l), \tag{4.2}$$

where $\nu\left(\sqrt{2K}\right)$ and $\mu\left(\sqrt{2K}\right)$ are nonnegative functions of K. According to [63], the values of $\nu\left(\sqrt{2K}\right)$ and $\mu\left(\sqrt{2K}\right)$ can be obtained given $K \in [0, 10]$. In the case of $0 < K \le 10$, $\nu\left(\sqrt{2K}\right)$ and $\mu\left(\sqrt{2K}\right)$ are given by

$$\mu\left(\sqrt{2K}\right) = 2.174 - 0.592\sqrt{2K} + 0.593\left(\sqrt{2K}\right)^2 - 0.092\left(\sqrt{2K}\right)^3 + 0.005\left(\sqrt{2K}\right)^4,$$

$$\nu\big(\sqrt{2K}\big) = -0.840 + 0.372\sqrt{2K} - 0.74\big(\sqrt{2K}\big)^2 + 0.083\big(\sqrt{2K}\big)^3 - 0.004\big(\sqrt{2K}\big)^4.$$

In the case of $K = 0$, $\mu_0 = 2$ and $\nu_0 = -\ln 2$.

In both cases, we have $\nu\big(\sqrt{2K}\big) < -1$ and $\mu\big(\sqrt{2K}\big) \geq 2$, and the convexity/concavity of $\tilde{Q}(l)$ can be further evaluated. This is critical to the development of the bounds of the UAV connectivities in the rest of this chapter. To evaluate the convexity/concavity of $\tilde{Q}(l)$, the second-order derivative of $\tilde{Q}(l)$ is first given by

$$\frac{d^2\tilde{Q}(l)}{dl^2} = \Big[(\tau_1\tau_2\tau_3)^2 l^{2\tau_3-2} - \tau_1\tau_2\tau_3(\tau_3-1)l^{\tau_3-2}\Big]e^{-\tau_1\tau_2 l^{\tau_3}},$$

where, for notation simplicity, $\tau_1 = e^{\nu(\sqrt{2K})}$, $\tau_2 = \left(\frac{2\sigma^2\rho_{\text{th}}(1+K)}{P}\right)^{\frac{1}{2}\mu(\sqrt{2K})}$, and $\tau_3 = \frac{1}{2}\alpha\mu\left(\sqrt{2K}\right)$.

Clearly, the sign of $\frac{d^2\tilde{Q}(l)}{dl^2}$ solely depends on $\big[(\tau_1\tau_2\tau_3)^2 l^{2\tau_3-2} - \tau_1\tau_2\tau_3(\tau_3-1)l^{\tau_3-2}\big]$. In the case that $l < l_{\text{th}} \triangleq \sqrt[\tau_3]{\frac{\tau_3-1}{\tau_1\tau_2\tau_3}}$, $\frac{d^2\tilde{Q}(l)}{dl^2} < 0$ and $\tilde{Q}(l)$ is concave with respect to l. In the case that $l \geq l_{\text{th}}$, $\frac{d^2\tilde{Q}(l)}{dl^2} \geq 0$ and $\tilde{Q}(l)$ is convex. Note that the value of l_{th} depends on the transmit SNR, i.e., $\frac{P}{\sigma^2}$, and grows quickly with the SNR, as demonstrated in Fig. 4.2. Under the typical parameter settings (as studied in this chapter), l_{th} is large and close to $2r$. For the analysis of the connectivity of a UAV to the rest of the UAVs, $l \leq l_{\text{th}}$ typically holds, and $\tilde{Q}(l)$ provides a good approximation to $Q(l)$. For the analysis of the broadcast connectivity of a UAV, $l > l_{\text{th}}$ typically holds, and $\tilde{Q}(l) < Q(l)$, as shown in Fig. 4.2. As will be discussed in Section 4.3.2, our analysis based on $\tilde{Q}(l)$ provides an upper bound for the broadcast connectivity under the typical settings. The approximation of $Q(l)$ to $\tilde{Q}(l)$ with $\tilde{Q}(l) < Q(l)$ would not violate the analysis of the upper bound.

We assume that all the UAVs have independent trajectories following a ST Mobility Model [59, 60]. The model decouples the movement of a UAV between the horizontal directions, i.e., along the x- and y-axes, and the vertical direction, i.e.,

along the z-axis [59].

On the horizontal plane, the UAV can randomly choose a turn center to circle around at a constant speed until the next turn center is identified. The duration of the UAV circling around a turn center is exponentially distributed. The next turn center is picked up on the line perpendicular to the instantaneous heading direction of the UAV. This ensures the smoothness of the flight trajectories. Furthermore, the 3D ST mobility model assumes that the inverse of every turn radius, i.e., $\frac{1}{r}$, follows a zero-mean Gaussian distribution with a small variance ($\frac{1}{r} > 0$ indicates right turns and $\frac{1}{r} < 0$ indicates left turns). In the vertical direction, i.e., along the z-axis, the UAV is assumed to maintain a constant acceleration while circling around a turn center for a random duration. The speed along the z-axis and the altitude can vary [59]. The other parameters of the model can be estimated from experimental measurements.

It has been proved in [60] that the 3D ST mobility model has a uniform stationary distribution of the UAV position within the 3D sphere. As a result, the N UAVs are independently and uniformly distributed within the sphere at any time instant. Different speeds of the UAVs would not affect the uniform distributions of the UAVs' positions. Therefore, the connectivity analysis based on *i.i.d.* positions of all UAVs is applicable to more general settings with different speeds of the UAVs.

4.3 Connectivity of the UAV Swarms

In this section, we study the distribution of the minimum distance from a UAV to any other UAVs, and evaluate the connectivity of the UAV. We also study the minimum and maximum distances of any pair of UAVs within the swarm, so that we are able to evaluate the best-case connectivity of the entire swarm and its broadcast connectivity.

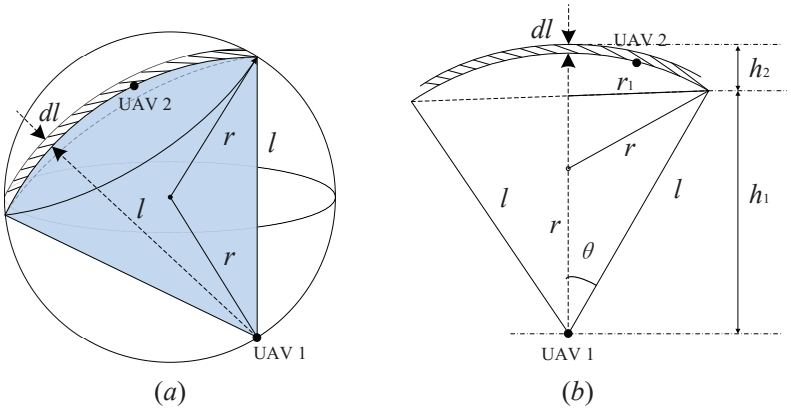


Figure 4.3 : Two UAVs in the spherical region (Special case: UAV 1 is located on the boundary of the spherical region).

4.3.1 Connectivity of Individual UAVs

The PDF of l, the Euclidean distance between a pair of UAVs in the 3D sphere with radius r, as illustrated in Fig. 4.3, denoted by $f_L(l)$, can be evaluated by employing the Crofton Fixed Point Theorem [66], as stated in Lemma 1 in Chapter 3.

Consider that a total number of N UAVs independently fly within the sphere, all following the ST mobility model in an uncoordinated fashion. Let L_i, $i = 1, \cdots, N-1$, collect the Euclidean distances from an arbitrarily selected UAV to the other $(N-1)$ UAVs; and assume that L_i are *i.i.d.* random variables. Let l_1 denote the shortest of the distances:

$$l_1 = \min_{i=1,\cdots,N-1} \{L_i\}. \tag{4.3}$$

The expectation of l_1 can be obtained as follows.

Lemma 2. *Suppose that N UAVs are randomly and independently distributed within the 3D sphere with radius r, then the expectation of the shortest of distances between an arbitrarily selected UAV to the other $(N-1)$ UAVs, i.e., $\mathbb{E}[l_1]$, can be approximately given by*

$$\mathbb{E}[l_1] \approx \frac{\Gamma(\frac{4}{3})\Gamma(N)}{\Gamma(N+\frac{1}{3})} r. \tag{4.4}$$

Proof. The proof was provided in section 3.4, Chapter 3. □

By exploiting Lemma 2 and the Jensen's inequality, we are able to establish the following theorem, namely, Theorem 1, on the outage probability of a randomly selected UAV flying a random 3D trajectory with smooth turns.

Theorem 2. *Suppose that N UAVs fly random trajectories with smooth turns in a 3D spherical region with Rician fading, the outage probability of the closest UAV pair satisfies*

$$\begin{cases} \mathbb{E}\big[P_{\text{out}_1}\big] \geq P^*_{\text{out1}}, \text{if } \mathbb{E}[l_1] < l_{\text{th}} \\ \mathbb{E}\big[P_{\text{out}_1}\big] \leq P^*_{\text{out1}}, \text{if } \mathbb{E}[l_1] \geq l_{\text{th}}, \end{cases} \tag{4.5}$$

where $l_{\text{th}} = \sqrt[\tau_3]{\frac{\tau_3 - 1}{\tau_1 \tau_2 \tau_3}}$, $\tau_1 = e^{\nu(\sqrt{2K})}$, $\tau_2 = \left(\frac{2\sigma^2 \rho_{\text{th}}(1+K)}{P}\right)^{\frac{1}{2}\mu(\sqrt{2K})}$, $\tau_3 = \frac{1}{2}\alpha\mu\left(\sqrt{2K}\right)$, *and*

$$P^*_{\text{out1}} = 1 - \exp\left[- e^{\nu(\sqrt{2K})} \times \left(\frac{2\sigma^2 \rho_{\text{th}}(1+K)\Gamma(\frac{4}{3})^{\alpha}\Gamma(N)^{\alpha} r^{\alpha}}{\Gamma(N+\frac{1}{3})^{\alpha} P} \right)^{\frac{1}{2}\mu\left(\sqrt{2K}\right)} \right].$$

The transmit power of the UAV that guarantees the connectivity of the UAV can be given by

$$\begin{cases} P \geq P^*_1, \text{if } \mathbb{E}[l_1] < l_{\text{th}} \\ P \leq P^*_1, \text{if } \mathbb{E}[l_1] \geq l_{\text{th}}, \end{cases} \tag{4.6}$$

where $P^*_1 = \frac{\left[-e^{\nu(\sqrt{2K})} \ln(1 - P^*_{\text{out}_1})\right]^{\frac{2}{\mu(\sqrt{2K})}} \Gamma(N+\frac{1}{3})^{\alpha}}{2\rho_{\text{th}}\sigma^2(1+K)\Gamma(\frac{4}{3})^{\alpha}\Gamma(N)^{\alpha} r^{\alpha}}$.

Proof. See Appendix 4.7.1. □

Note that the derivation of (4.29) to (4.32) is based on the case where N is very large, but not necessarily approaches infinite. (4.29) is of practical interest, as $\mathbb{E}[l_1] < l_{\text{th}}$ remains active under the typical parameter settings, as noted in Section 4.2 and will be discussed in Section 4.5. It provides the lower bound for the

outage probability in typical network configurations. Moreover, $\tilde{Q}(l)$ exhibits weak curvature, especially in the case that $l < l_{\text{th}}$, as shown in Fig. 4.2. In this sense, the lower bound (4.29) also provides a good approximation to the outage probability, as will be shown in Section 4.5.

4.3.2 Broadcast Connectivity of the UAV Swarm

We proceed to evaluate the largest distance between any pair of the N UAVs within the 3D sphere V. The largest distance is denoted by $l_2 = \max_{i=1,\cdots,N-1}\{L_i\}$. The expectation of l_2 can be obtained as follows.

Lemma 3. *Suppose that N UAVs are randomly and independently distributed within the 3D sphere with radius r. Then the expectation of the largest of the distances between any pair of UAVs, denoted by $\mathbb{E}[l_2]$, can be approximately given by*

$$\mathbb{E}[l_2] \approx 2r\left[1-\exp(-6N^2r^3)\right] - \sqrt[3]{\frac{4}{3}}N^{-\frac{2}{3}}\gamma\left(\frac{4}{3}, 6N^2r^3\right), \tag{4.7}$$

where $\gamma(a,b) = \int_0^b e^{-t}t^{a-1}dt$ is the incomplete Gamma function. In the case $N \to \infty$, $\mathbb{E}[l_2] \to 2r$.

Proof. The proof was provided in section 3.4, Chapter 3. □

Based on Lemma 3 and the Jensen's inequality, we are able to establish the following theorem on the outage probability of the furthest UAV pair in the 3D sphere.

Theorem 3. *Suppose that N UAVs fly random trajectories with practical smooth turns in a 3D spherical region with Rician fading, the outage probability of any pair of UAVs satisfies*

$$\begin{cases} \mathbb{E}\left[P_{\text{out}_2}(l_2)\right] \geq P^*_{\text{out}2}\left(\mathbb{E}[l_2]\right), \mathbb{E}[l_2] < l_{\text{th}} \\ \mathbb{E}\left[P_{\text{out}_2}(l_2)\right] \leq P^*_{\text{out}2}\left(\mathbb{E}[l_2]\right), \mathbb{E}[l_2] \geq l_{\text{th}}, \end{cases} \tag{4.8}$$

where $l_{\text{th}} = \sqrt[\tau_3]{\frac{\tau_3-1}{\tau_1\tau_2\tau_3}}$, $\tau_1 = e^{\nu(\sqrt{2K})}$, $\tau_2 = \left(\frac{2\sigma^2\rho_{\text{th}}(1+K)}{P}\right)^{\frac{1}{2}\mu(\sqrt{2K})}$, $\tau_3 = \frac{1}{2}\alpha\mu\left(\sqrt{2K}\right)$, *and*

$$P^*_{\text{out2}} = 1 - \exp\left[- e^{\nu\left(\sqrt{2K}\right)} \times \left(\frac{2\sigma^2\rho_{\text{th}}(1+K)\mathbb{E}\left[l_2\right]^{\alpha}}{P}\right)^{\frac{1}{2}\mu\left(\sqrt{2K}\right)} \right].$$

The transmit power of the UAV, which can guarantee the connectivity of the UAV, is given by

$$\begin{cases} P < P_2^*, \text{if } \mathbb{E}[l_2] < l_{\text{th}} \\ P \geq P_2^*, \text{if } \mathbb{E}[l_2] \geq l_{\text{th}}, \end{cases} \tag{4.9}$$

where $P_2^* = \frac{\left[-e^{\nu(\sqrt{2K})}\ln(1-P^*_{\text{out}_2})\right]^{\frac{2}{\mu(\sqrt{2K})}}}{2\rho_{\text{th}}\sigma^2(1+K)\mathbb{E}[l_2]^{\alpha}}$.

Proof. See Appendix 4.7.2. □

Different from the connectivity of individual UAVs in Sections 4.3.1, the case of $\mathbb{E}[l_2] \geq l_{\text{th}}$ is dominant in the study of the broadcast connectivity under typical parameter settings. This is due to the fact that as the average maximum distance between any pair of UAVs in a UAV swarm, $\mathbb{E}[l_2]$, is typically close to $2r$. To this end, (4.33) can be adopted as the upper bound for the outage probability of broadcast in a UAV swarm, as will be shown in Section 4.5.

Remark 1. *From Theorem 2 and Theorem 3, we can find that both the average one-hop outage probability and broadcast outage probability of the UAV decrease with the growth of N, since the distance between UAVs decreases with an increasing number of UAVs in the swarm. The outage probabilities also decrease with the growth of K, this is because the LoS path becomes increasingly dominant and reduces the outage.*

4.4 Connectivity of the UAV Swarms under the ground Interference

Aerial receivers are vulnerable to the interference from ground transmitters [61, 73]. This scenario can be analyzed by extending Lemma 1 in chapter 3 as such, that the ground station is fixed on the surface of the aforementioned 3D sphere while the UAV flies within the 3D sphere. Let l_I denote the distance between a designated UAV within the sphere and the ground transmitter. The expectation of l_I, $\mathbb{E}[l_I]$, can be obtained as follows.

Lemma 4. *Suppose that N UAVs are randomly and independently distributed within the 3D sphere with radius r, and the ground transmitter is located on the surface of the sphere. The expectation of the distance between a randomly selected UAV within the sphere and the ground transmitter, i.e., $\mathbb{E}[l_I]$, can be approximately given by*

$$\mathbb{E}[l_I] = \frac{6}{5}r. \tag{4.17}$$

Proof. The proof was provided in section 3.4, Chapter 3. □

4.4.1 Outage Probability under Interference from Ground Transmitter

We assume that the interference link experiences the Rician fading. We analyze the interference from a fixed ground station to UAVs flying random 3D trajectories with smooth turns.

The received signal at each of the pair of UAVs can be written as

$$y = \sqrt{P}h(t)s(t) + \sqrt{P_I}h_I(t)s(t) + n(t), \tag{4.18}$$

where P_I is the transmit power of the ground transmitter, and h_I is the channel fading coefficient between the ground transmitter and the UAV.

The SINR, denoted by ζ, can be represented as

$$\zeta = \frac{Pl^{-\alpha}|h|^2}{P_I {l_I}^{-\alpha_I}|h_I|^2 + \sigma^2}. \tag{4.19}$$

Accordingly, the outage probability can be given by

$$P'_{\text{out}} = \Pr\left(\zeta \le \rho_{\text{th}}\right) = \Pr\left(\frac{Pl^{-\alpha}|h|^2}{P_I {l_I}^{-\alpha_I}|h_I|^2 + \sigma^2} \le \rho_{\text{th}}\right) \tag{4.20a}$$

$$= \Pr\left(Pl^{-\alpha}|h|^2 - P_I {l_I}^{-\alpha_I}\rho_{\text{th}}|h_I|^2 \le \sigma^2\rho_{\text{th}}\right) = \Pr\left(Z \le \sigma^2\rho_{\text{th}}\right), \tag{4.20b}$$

where (4.20b) is obtained by setting $X \triangleq Pl^{-\alpha}|h|^2$, $Y \triangleq P_I {l_I}^{-\alpha_I}\rho_{\text{th}}|h_I|^2$, and $Z \triangleq X - Y$; and α_I is the path loss exponent between the UAV and the ground station.

Theorem 4. *Suppose that the channel coefficient h and h_I follow the Rician distribution with parameter K and K_I, respectively. The outage probability can be obtained as $P'_{\text{out}} = \int_0^{\rho_{\text{th}}} f_Z(z)dz$,*

$$f_Z(z) = \int_0^{\infty} f_X(z+y) f_Y(y) dy \tag{4.21a}$$

$$= \int_0^{\infty} \frac{1+K}{\Omega_x} \exp\left(-K - \frac{1+K}{\Omega_x}(z+y)\right) I_0\left(2\sqrt{\frac{K(1+K)(z+y)}{\Omega_x}}\right) \frac{1+K_I}{\Omega_y}$$

$$\times \exp\left(-K_I - \frac{1+K_I}{\Omega_y}y\right) I_0\left(2\sqrt{\frac{K_I(1+K_I)}{\Omega_y}y}\right) dy \tag{4.21b}$$

$$= \frac{(1+K)(1+K_I)\exp(-K-K_I)}{\Omega_x\Omega_y} \exp\left(-\frac{1+K}{\Omega_x}z\right) \int_0^{\infty} \left\{\exp\left[-\left(\frac{1+K}{\Omega_x} + \frac{1+K_I}{\Omega_y}\right)y\right]\right.$$

$$\left. \times \sum_{k=0}^{\infty}\left[\frac{K_I^k(1+K_I)^k y^k}{(k!)^2} F\left(-k,-k;-1;\frac{K(1+K)\Omega_y}{K_I(1+K_I)\Omega_x}\right)\right]\right\} dy \tag{4.21c}$$

$$= \frac{(1+K)(1+K_I)\exp(-K-K_I)}{\Omega_x\Omega_y} \exp\left(-\frac{1+K}{\Omega_x}z\right)$$

$$\times \sum_{k=0}^{\infty}\left\{\frac{K_I^k(1+K_I)^k\Omega_x^k\Omega_y^k}{k![(1+K)\Omega_y + (1+K_I)\Omega_x]^k} F\left(-k,-k;-1;\frac{K(1+K)\Omega_y}{K_I(1+K_I)\Omega_x}\right)\right\}, \tag{4.21d}$$

where $\Omega_x = Pl^{-\alpha}$ and $\Omega_y = P_I {l_I}^{-\alpha_I}\rho_{\text{th}}$; (4.21c) is based on the identity product that

$I_0\left(2\sqrt{\frac{K(1+K)(z+y)}{\Omega_x}}\right) I_0\left(2\sqrt{\frac{K_I(1+K_I)}{\Omega_y}y}\right) = \sum_{k=0}^{\infty}\left[\frac{K_I^k(1+K_I)^k y^k}{(k!)^2} F\left(-k,-k;-1;\frac{K(1+K)\Omega_y}{K_I(1+K_I)\Omega_x}\right)\right]$ *[69, 8.442]; and* $F(\cdot)$ *is the hypergeometric function.*

It is difficult to derive the closed-form expression for P'_{out} based on (4.21), and the results can hardly provide useful insights. On the other hand, a ground interference station is typically far away from UAVs. It can be indoors. There is unlikely to be a direct path between the ground station and the UAV. Moreover, the link between the UAV and the ground transmitter is susceptible to body blockage. Therefore, we can assume that the fading follows Rayleigh distribution, i.e., $K_I = 0$. In this case, the outage probability can be obtained as follows.

Theorem 5. *Suppose that the channel coefficient* h *follows the Rician distribution with parameter* K*, and the channel coefficient* h_I *follows the Rayleigh distribution, i.e.,* $|h_I|^2 \sim \exp(1)$ *(i.e,* $K_I = 0$*). The outage probability in the presence of the interference from the ground transmitters, can be given by*

$$P'_{\text{out}} = 1 - Q\left(\sqrt{2K}, \sqrt{\frac{2(1+K)\sigma^2\rho_{\text{th}}}{\Omega_x}}\right) + \Omega_m \exp\left(-K + K\Omega_m\right) \exp\left(\frac{\sigma^2\rho_{\text{th}}}{\Omega_y}\right) \times Q\left(\sqrt{2K\Omega_m}, \sqrt{\frac{2(1+K)\sigma^2\rho_{\text{th}}}{\Omega_x\Omega_m}}\right), \tag{4.22}$$

which is upper bounded by

$$P'_{\text{out}} \leq P_{\text{out}} + \Omega_m \exp\left[-K + K\Omega_m + \frac{\sigma^2\rho_{\text{th}}}{\Omega_y} - e^{\nu\left(\sqrt{2K}\right)}\left(\frac{2(1+K)\sigma^2\rho_{\text{th}}}{\Omega_x\Omega_m}\right)^{\frac{1}{2}\mu\left(\sqrt{2K}\right)}\right] \triangleq \Phi\left(l, l_I\right), \tag{4.23}$$

where $\Omega_m = \frac{(1+K)\Omega_y}{\Omega_x + (1+K)\Omega_y}$ *for* $0 \leq \Omega_m \leq 1$.

Proof. See Appendix 4.7.4. □

Corollary 3. *In the case of* $K = 0$ *and* $K_I = 0$*, the outage probability in the*

presence of interference from the ground transmitter is upper bounded by

$$P'_{\text{out}} \leq 1 - \frac{\Omega_x}{\Omega_x + \Omega_y} \exp\left(-\frac{\sigma^2 \rho_{\text{th}}}{\Omega_x}\right) \triangleq \Phi_0\left(l, l_I\right), \tag{4.24}$$

where $\Phi_0\left(l, l_I\right)$ *is the outage probability as a function of* l/l_I*, and*

$$\mathbb{E}_{l,l_I}\left\{\Phi_0\left(l, l_I\right)\right\} \approx \Phi_0\left(\mathbb{E}\left[l\right], \mathbb{E}\left[l_I\right]\right). \tag{4.25}$$

Proof. See Appendix 4.7.5. □

4.4.2 Connectivity analysis

The connectivity of a UAV can be analyzed in the presence of the interference from the ground transmitter:

4.4.2.1 Connectivity of Individual UAVs

Based on Corollary 3, we can establish the bounds for the outage probability of an arbitrary UAV. The upper bound for the expectation of the outage probability, denoted by $\mathbb{E}\left[P'_{\text{out}_1}\right]$, can be given by

$$\mathbb{E}_{l_1,l_I}\left[P'_{\text{out}_1}\right] \leq \mathbb{E}_{l_1,l_I}\left[\Phi_0(l_1, l_I)\right] \tag{4.26a}$$

$$\approx \Phi_0\left[\mathbb{E}(l_1), \mathbb{E}(l_I)\right] = 1 - \Omega^*_{m_1} \exp\left(-\frac{\sigma^2 \rho_{\text{th}} \Gamma(\frac{4}{3})^\alpha \Gamma(N)^\alpha r^\alpha}{\Gamma(N+\frac{1}{3})^\alpha P}\right) \triangleq P'^*_{\text{out}_1}, \tag{4.26b}$$

where $\Omega^*_{m_1} = \frac{1}{1+\frac{P}{P_I \rho_{\text{th}}}\left(\frac{6}{5}\right)^{\alpha_I}\left(\Gamma\left(N+\frac{1}{3}\right)/\Gamma\left(\frac{4}{3}\right)\Gamma(N)\right)^\alpha r^{\alpha_I/\alpha}}$; The approximation in (4.26b) is obtained from Corollary 3; and $\mathbb{E}(l_I) \approx \frac{6}{5}r$ is based on Lemma 4.

4.4.2.2 Broadcast Connectivity of the UAV Swarm

The upper bound for the expectation of the outage probability between the furthest pair of UAVs, denoted by $\mathbb{E}\left[P'_{\text{out}_2}\right]$, can also be evaluated, as given by

$$\begin{aligned}\mathbb{E}_{l_2,l_I}\left[P'_{\text{out}_2}\right] &\leq \mathbb{E}_{l_2,l_I}\left[\Phi_0(l_2,l_I)\right] \approx \Phi_0\left[\mathbb{E}(l_2),\mathbb{E}(l_I)\right] \\ &= 1-\Omega^*_{m_2}\exp\left(-\frac{\sigma^2\rho_{\text{th}}\mathbb{E}[l_2]^{\alpha}}{P}\right) \triangleq P'^*_{\text{out}_2},\end{aligned} \tag{4.27}$$

where $\Omega^*_{m_2} = \frac{1}{1+\frac{P}{P_I\rho_{\text{th}}}\left(\frac{6}{5}r\right)^{\alpha_I}\mathbb{E}[l_2]^{-\alpha}}$.

Remark 2. *From Corollary 3, we can obtain the relationship between the outage probabilities in the presence and absence of the interference from the ground transmitter, as follows:*

$$\Phi_0\left(l,l_I\right) = 1-\left[1-\frac{\Omega_y}{\Omega_x+\Omega_y}\exp\left(\frac{\sigma^2\rho_{\text{th}}}{\Omega_y}\right)\right]\tilde{Q}(l) = P_{\text{out}}+\frac{\Omega_y}{\Omega_x+\Omega_y}\exp\left(\frac{\sigma^2\rho_{\text{th}}}{\Omega_y}\right)\tilde{Q}(l). \tag{4.28}$$

With Rayleigh fading channels considered both between UAVs and between UAVs and the ground transmitter, (4.28) *provides the upper bound outage probability for typical UAV scenario where there is an LoS link between the UAVs, and the channels are typically Rician. We note that a Rician fading channel has the same distribution as a Rayleigh fading channel with the only difference of a positive mean. As a result, the desired signal between the UAVs is expected to have the same distribution in the Rician channel as in the Rayleigh channel, except for the mean. To this end, the above analysis under the Rayleigh channels provides the upper bound for the outage probability in the Rician channels.*

4.5 Simulation and Evaluation

In this section, we conduct extensive simulations to validate the accuracy of our analytical results for the connectivity of uncoordinated UAV swarms in a 3D space.

Table 4.1 : Simulation parameters

Parameter	Value
Transmit power of the ground transmitter P_I	20 dBm
Noise power σ^2	-80 dBm
Path loss exponent α	3 [70]
Rician factor K	0, 2 dB, 5 dB
SNR/SINR threshold ρ_{th}	0, 5, 10 dB

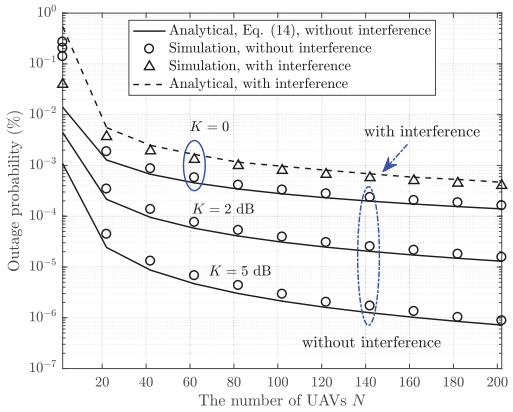
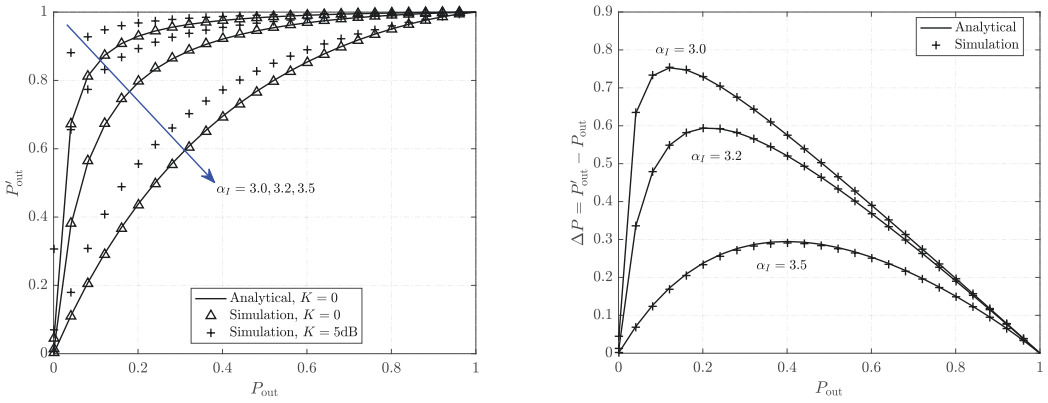


Figure 4.4 : The outage probability of an arbitrary UAV vs. the number of UAVs, N, under different Rician factors, where $r = 500$ m, $\rho_{\text{th}} = 5$ dB, and $\alpha_I = 3.5$.

The radius of the space is $r = 500$ m, the number of UAVs is up to 500, the transmit power of a UAV is $P = 20$ dBm, and the transmit power of the ground transmitter is $P_I = 20$ dBm; unless otherwise specified. As mentioned in Section 6.2.1, the ST mobility model is adopted for the UAVs. Other system parameters are listed in Tab. 4.1 with reference to [72, 70].

4.5.1 Connectivity of individual UAVs

Fig. 4.4 evaluates the connectivity of an arbitrarily selected UAV in the UAV swarm in the presence and absence of the interference from the ground transmitter, where the outage probability of link l_1 against the total number of UAVs, N, is plotted under different Rician factors K. The Rician factor $K = 0$ captures the case



(a) P'_{out} vs. P_{out} (b) ΔP vs. P_{out} ($K = 0$)

Figure 4.5 : The outage probability in the presence of interference from the ground transmitter vs. the outage probability in the absence of interference from the ground transmitter under different α_I, where $r = 500$, $N = 50$, $K_I = 0$, and $\alpha = 3$.

where there is no LoS path and the channel becomes a Rayleigh fading channel. We also use $K = 5$ dB to capture the case where there are both LoS path and NLoS paths between a pair of UAVs. The NLoS is assumed to be resulted from body blockage of the UAVs and the reflection and scattering stemming from other UAVs.

As shown in Fig. 4.4, the analytical result (4.29) provides lower bounds for the corresponding simulation results, both with and without interferences from the ground transmitter, because $\mathbb{E}[l_1] < l_{\text{th}}$ under the simulation settings, as discussed in Section 4.3.1. With the increase of N, the lower bound can be asymptotically tight and become indistinguishably close to the simulation results. This is due to the fact that $\tilde{Q}(l)$ exhibits weak curvature and the gap between the lower bound (4.29) and the actual outage probability is small and increasingly negligible, as N grows. For small N, e.g., $N = 2$, the analytical results of (4.29) are less accurate due to the approximation (4.4). From the figure, we see that the outage probability of an individual UAV decreases with the increasing number of UAVs in the swarm N, and decreases with the growth of K, since the LoS path becomes increasingly dominant and reduces the outage.

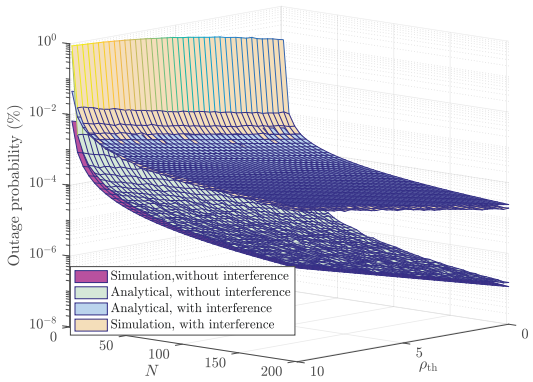


Figure 4.6 : The outage probability of an arbitrary UAV vs. the number of UAVs under different SNR/SINR thresholds, where $K = K_I = 0$ and $r = 500$ m.

Fig. 4.5 plots the outage probability of an arbitrarily selected UAV in the presence of the interference from the ground transmitter, P'_{out}, versus the outage probability in the absence of the interference, P_{out}. Both the analytical bounds, i.e., (4.29) and (4.26), and the simulation results are provided. We can see in fig. 4.5(a) our analysis under Rayleigh fading channels, i.e., (4.26), serves the lower bound for the outage probability under Rician fading channels, in the presence of the ground interferences. We can see that P'_{out} increases with P_{out}. However, the difference between P'_{out} and P_{out}, i.e., ΔP, first increases and then decreases with the growth of P_{out}, as shown in Fig. 4.5(b). We can draw the conclusion that the interference from the ground transmitters is detractive to the connectivity of the UAVs, especially when UAVs fly at low elevations, i.e., $\alpha_I \to \alpha$, and/or the UAVs have good channel conditions, i.e., P_{out} is small.

Fig. 4.6 depicts the outage probability of an arbitrarily selected UAV both in the presence and the absence of interference from the ground transmitter, where the number of UAVs, N, and the SNR/SINR thresholds, ρ_{th}, vary. We can see that the analytical result (4.29) provides increasingly tight upper bounds for the simulation results, as N increases. We also see that the outage probability decreases with the

growth of N, since the distance between UAVs decreases with an increasing number of UAVs in the swarm, and becomes increasingly tight and accurate, as ρ_{th} grows.

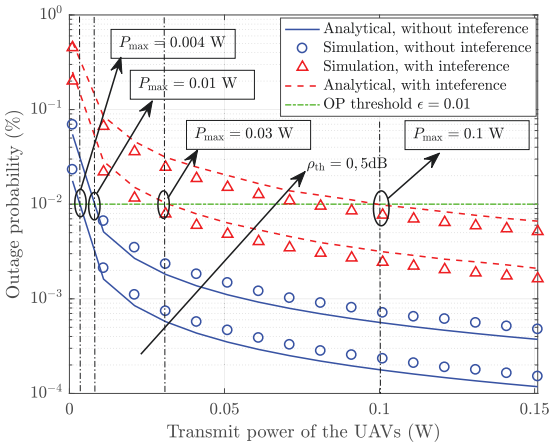


Figure 4.7 : The outage probability of an arbitrary UAV vs. the transmit power of UAVs for different values of SNR threshold, where $r = 500$ m, $N = 50$, $\alpha = 3$,$\alpha_I = 3.5$, and the Rician factor is $K = 0$.

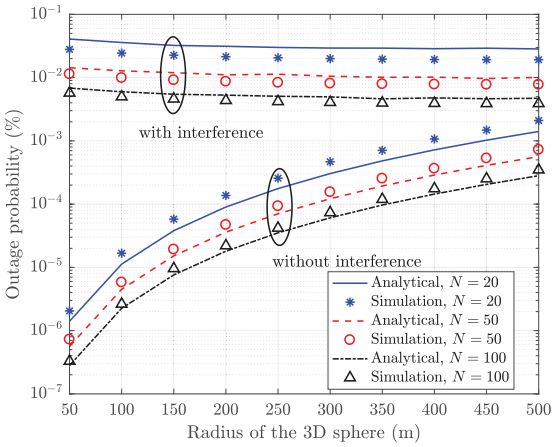
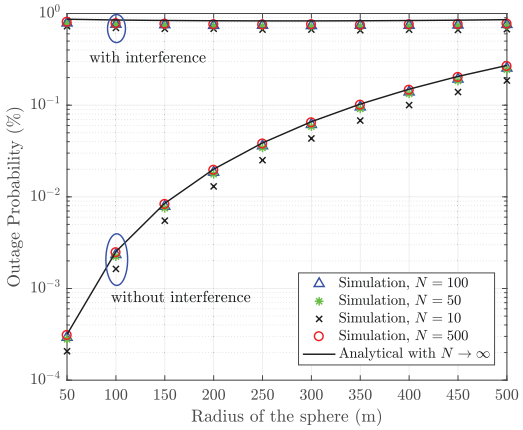


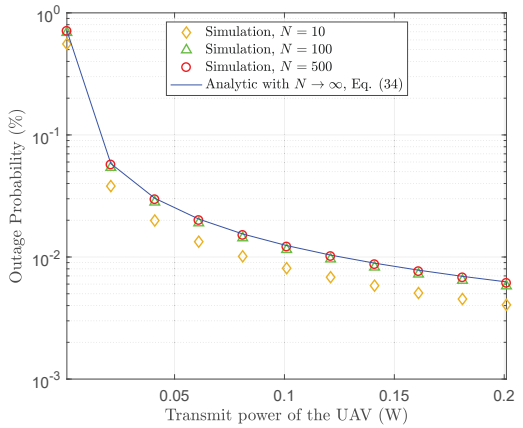
Figure 4.8 : The outage probability of an arbitrary UAV vs. the radius of the sphere r, under different total numbers of UAVs, where the Rician factor $K = 0$, $P = 0.1$ W and $\rho_{\text{th}} = 5$ dB.

In Fig. 4.7, the outage probabilities of the arbitrary UAV in both the presence and absence of interferences from the ground transmitter are plotted against the increasing transmit power of the UAVs, P, under different SNR thresholds ρ_{th}. We can see that the outage decreases with the growth of P. With the growth of ρ_{th}, the analytical result (4.29) becomes increasingly accurate. We also highlight the transmit powers required to achieve the minimum outage probability of 10^{-2} under different settings of ρ_{th}. The maximum transmit powers required, as can be evaluated in Sections 4.3 and 4.4, are consistent with the simulation results.

Fig. 4.8 plots the outage probability of an arbitrarily selected UAV both with and without interference from the ground transmitter, as the coverage of the 3D sphere increases. The figure shows the probability under different numbers of uncoordinated UAVs in the swarm, i.e., N. We can see that our analytical lower bound, (4.29),



(a) The outage probability of broadcast vs. the radius of the 3D space, r, with the path loss $\alpha_I = 3.2$, the Rician factor $K = K_I = 0$ and $\rho_{\text{th}} = 5$ dB.



(b) The outage probability of broadcast vs. the transmit power of UAVs, P, under different numbers of UAVs, where $r = 500$ m, $\alpha_I = 3.2$, $K = K_I = 0$ and $\rho_{\text{th}} = 5$ dB.

Figure 4.9 : The outage probability between the furthest pair of UAVs in the UAV swarm.

and upper bound, (4.44), can be increasingly tight with the enlarging size of the 3D sphere (or in other words, the coverage area of the UAVs). We also see that, with an increasing number of UAVs, the analytical upper bound of the outage probability also becomes increasingly accurate. To this end, the lower bound (4.29) and upper bound (4.44) are shown to be very useful for quantifying the connectivity of a dense uncoordinated UAV swarm over a large 3D space.

4.5.2 Broadcast Connectivity of the UAV Swarm

Figs. 4.9(a) and 4.9(b) plot the analytical results of (4.33) with the growing coverage of the 3D sphere r and the transmit power of a UAV, P, respectively. Different numbers of UAVs are simulated, i.e., $N = 10, 50, 100, 500$. We can see that the analytical results, evaluated under the assumption of $N \to \infty$, provide tight upper bounds for the outage probability, especially when N is large. The assumption of the analysis is asymptotically effective. Particularly, the simulation results for $N = 500$ against both P and r are closer to the analytical results developed under the assumption for $N \to \infty$, than the simulation results of $N = 10$ or 100. The reason for (4.33) being the upper bound of the broadcast connectivity (as opposed to (4.35) being the lower bound) is due to the fact that $\mathbb{E}[l_2]$, which is typically close to $2r$, is larger than l_{th}, and therefore (4.33) provides the upper bound for the outage probability of broadcast in the UAV swarm.

4.6 Conclusion

In this chapter, we developed closed-form expressions for the outage probability of UAVs (or in other words, the one-hop connectivity of a UAV and the broadcast connectivity of the UAV) in an uncoordinated UAV swarm, where the UAVs fly within a 3D sphere with practical smooth turns both in the absence and presence of ground interference. Our analysis was based on comprehensive 3D geometric interpretations which translate the trajectories to steady-state spatial distributions of the UAVs. Extensive simulations confirm that our analyses are accurate and provide tight performance bounds for the connectivity of a dense uncoordinated UAV swarm in a large 3D space.

4.7 Appendices

4.7.1 Proof of Theorem 2.

As discussed in Section 4.2.1, $\tilde{Q}\big(l\big)$ decays exponentially with the growth of the distance l, and exhibits concavity for $l < l_{\rm th}$ and convexity for $l \geq l_{\rm th}$. According to Lemma 2 and the concavity/convexity of $\tilde{Q}\big(l\big)$, the Jensen's inequality can be exploited to develop the bounds for the outage probability of the UAV of interest.

In the case that $\mathbb{E}[l_1] < l_{\rm th}$, the lower bound for the expectation of the outage probability of an arbitrarily selected UAV, denoted by $\mathbb{E}\big[P_{\rm out_1}\left(l_1\right)\big]$, is given by

$$\begin{aligned}
&\mathbb{E}\big[P_{\rm out_1}\left(l_1\right)\big] = 1 - \mathbb{E}\left[\tilde{Q}\big({l_1}^{\alpha}\big)\right] \geq 1 - \tilde{Q}\big(\mathbb{E}\left[l_1\right]^{\alpha}\big) \\
&= 1 - \exp\left[- e^{\nu\left(\sqrt{2K}\right)} \left(\frac{2\sigma^2 \rho_{\rm th}(1+K)\Gamma(\frac{4}{3})^{\alpha}\Gamma(N)^{\alpha} r^{\alpha}}{\Gamma(N+\frac{1}{3})^{\alpha} P} \right)^{\frac{1}{2}\mu\left(\sqrt{2K}\right)} \right] \\
&\triangleq P^{*}_{\rm out_1}, \text{ if } \mathbb{E}[l_1] < l_{\rm th},
\end{aligned} \tag{4.29}$$

where the inequality is based on the Jensen's inequality.

The connectivity of the UAV can be ensured at the probability no less than $(1 - P^{*}_{\rm out_1})$. Further, we can obtain the minimum transmit power of the UAV which guarantees the connectivity of the UAV, as given by

$$P \geq \frac{\left[- e^{\nu\left(\sqrt{2K}\right)} \ln(1 - P^{*}_{\rm out_1})\right]^{\frac{2}{\mu\left(\sqrt{2K}\right)}} \Gamma(N + \frac{1}{3})^{\alpha}}{2\rho_{\rm th}\sigma^2 \left(1 + K\right) \Gamma(\frac{4}{3})^{\alpha}\Gamma(N)^{\alpha} r^{\alpha}} \triangleq P^{*}_{1}, \text{if } \mathbb{E}[l_1] < l_{\rm th}. \tag{4.30}$$

In the case that $\mathbb{E}[l_1] \geq l_{\rm th}$, the upper bound for $\mathbb{E}\big[P_{\rm out_1}\big]$ is given by

$$\mathbb{E}\big[P_{\rm out_1}\big] \leq P^{*}_{\rm out_1}, \text{if } \mathbb{E}[l_1] \geq l_{\rm th}. \tag{4.31}$$

The maximum transmit power of the UAV, which is required to achieve the connec-

tivity of the UAV, can be given by

$$P \leq P_1^*, \text{if } \mathbb{E}[l_1] \geq l_{\text{th}}. \tag{4.32}$$

By combining (4.30) and (4.32), we establish (4.6).

4.7.2 Proof of Theorem 3.

As discussed in Sections 4.3.1, the Jensen's inequality can be exploited. Based on the concavity/convexity of $\tilde{Q}(\cdot)$, the lower and upper bounds for the expectation of the outage probability between the furthest pair of UAVs, $\mathbb{E}\big[P_{\text{out}_2}(l_2)\big]$, can be evaluated.

In the case that $\mathbb{E}[l_2] \geq l_{\text{th}}$, the upper bound for $\mathbb{E}\big[P_{\text{out}_2}(l_2)\big]$ can be derived as

$$\begin{aligned}\mathbb{E}\big[P_{\text{out}_2}(l_2)\big] &\leq 1 - Q\big(\mathbb{E}[l_2]^{\alpha}\big) \leq 1 - \tilde{Q}\big(\mathbb{E}[l_2]^{\alpha}\big) \\ &= 1 - \exp\left[- e^{\nu(\sqrt{2K})} \left(\frac{2\sigma^2 \rho_{\text{th}} (1+K) \mathbb{E}[l_2]^{\alpha}}{P} \right)^{\frac{1}{2}\mu(\sqrt{2K})} \right] \triangleq P_{\text{out}_2}^*(\mathbb{E}[l_2]),\end{aligned} \tag{4.33}$$

where $Q(l) > \tilde{Q}(l)$ for $l > l_{\text{th}}$ is used, as discussed in Section 4.2.1. The minimum transmit power that is required to achieve the broadcast connectivity at the probability $P_{\text{out}_3}^*$ is given by

$$P \geq \frac{\big[- e^{\nu(\sqrt{2K})} \ln(1 - P_{\text{out}_2}^*) \big]^{\frac{2}{\mu(\sqrt{2K})}}}{2\rho_{\text{th}} \sigma^2 (1+K) \mathbb{E}[l_2]^{\alpha}} \triangleq P_2^*. \tag{4.34}$$

In the case that $\mathbb{E}[l_2] < l_{\text{th}}$, the lower bound for $\mathbb{E}\big[P_{\text{out}_2}(l_2)\big]$ is given by

$$\mathbb{E}\big[P_{\text{out}_2}(l_2)\big] \geq P_{\text{out}_2}^*(\mathbb{E}[l_2]), \tag{4.35}$$

and the maximum transmit power of a UAV required to achieve the lower bound is P_2^*.

4.7.3 Proof of $\mathcal{X} - \mathbb{E}[\mathcal{X}] \longrightarrow 0$.

Let $\mathcal{X}$ in Corollary 3 be $\mathcal{X} = 1/\sum_{i=1}^{\theta} x_i$, where $x_i (i = 1, \cdots, \theta)$ is a sequence of positive square-integrable random variables which is not necessarily independent across i, and $\theta \to \infty$. Moreover, there exists $\varsigma > 0$, such that $\liminf_i \mathbb{E}[x_i] > \varsigma$.

According to the law of large numbers,

$$\frac{1}{\theta}\sum_{i=1}^{\theta} x_i - \frac{1}{\theta}\sum_{i=1}^{\theta} \mathbb{E}[x_i] \xrightarrow{a.s.} 0, \text{as } \theta \to \infty.$$

Since $\frac{1}{\theta}\sum_{i=1}^{\theta} \mathbb{E}[x_i]$ is bounded away from 0, we have

$$\frac{1}{\frac{1}{\theta}\sum_{i=1}^{\theta} x_i} - \frac{1}{\frac{1}{\theta}\sum_{i=1}^{\theta} \mathbb{E}[x_i]} \xrightarrow{a.s.} 0, \text{as } \theta \to \infty. \tag{4.36}$$

That is,

$$\mathbb{E}\left[\frac{1}{\frac{1}{\theta}\sum_{i=1}^{\theta} x_i}\right] - \frac{1}{\frac{1}{\theta}\sum_{i=1}^{\theta} \mathbb{E}[x_i]} \xrightarrow{a.s.} 0, \text{as } \theta \to \infty. \tag{4.37}$$

Using (4.36) minus (4.37), we can obtain

$$\frac{1}{\frac{1}{\theta}\sum_{i=1}^{\theta} x_i} - \mathbb{E}\left[\frac{1}{\frac{1}{\theta}\sum_{i=1}^{\theta} x_i}\right] \xrightarrow{a.s.} 0, \text{as } \theta \to \infty, \tag{4.38}$$

which means $\theta\mathcal{X} - \theta\mathbb{E}[\mathcal{X}] \xrightarrow{a.s.} 0, \text{as } \theta \to \infty$.

By recalling the definition of almost sure convergence: $\forall \varepsilon > 0$, there exists a θ_1 such that for $\theta_1 > \theta$,

$$\Pr\left(\left|\theta_1 \left(\mathcal{X} - \mathbb{E}[\mathcal{X}]\right)\right| < \varepsilon\right) = 1.$$

Hence,

$$\Pr\left(\left|\left(\mathcal{X} - \mathbb{E}[\mathcal{X}]\right)\right| < \varepsilon\right) = 1,$$

and therefore,

$$\mathcal{X} - \mathbb{E}[\mathcal{X}] \xrightarrow{a.s.} 0, \text{as } \theta \to \infty. \tag{4.39}$$

4.7.4 Proof of Theorem 5.

Given that h follows the Rician distribution with parameter K and $|h_I|^2 \sim \exp(1)$, the PDF of Z can be rewritten as

$$f_Z(z) = \int_0^\infty \frac{1+K}{\Omega_x} \exp\left(-K - \frac{1+K}{\Omega_x}(z+y)\right) I_0\left(2\sqrt{\frac{K(1+K)}{\Omega_x}(z+y)}\right) \frac{\exp\left(-\frac{y}{\Omega_y}\right)}{\Omega_y} dy \tag{4.40a}$$

$$= \frac{(1+K)\exp(-K)}{\Omega_x\Omega_y} \int_z^\infty \exp\left(-\frac{1+K}{\Omega_x}y_1\right) I_0\left(2\sqrt{\frac{K(1+K)y_1}{\Omega_x}}\right) \exp\left(-\frac{y_1 - z}{\Omega_y}\right) dy_1 \tag{4.40b}$$

$$= \frac{B\exp\left(-K+\frac{B}{2}\right)}{2K\Omega_y} \exp\left(\frac{z}{\Omega_y}\right) \times \int_{Az}^\infty \frac{1}{2}\exp\left(-\frac{y_2+B}{2}\right) I_0\left(\sqrt{By_2}\right) dy_2 \tag{4.40c}$$

$$= \frac{B\exp\left(-K+\frac{B}{2}\right)}{2K\Omega_y} \exp\left(\frac{z}{\Omega_y}\right) Q\left(\sqrt{B}, \sqrt{Az}\right), \tag{4.40d}$$

where (4.40b) is obtained by setting $y_1 = y + z$; (4.40c) is obtained by setting $y_2 = Ay_1 = \frac{2[\Omega_x+(1+K)\Omega_y]}{\Omega_x\Omega_y}y_1$ and $B = \frac{2K(1+K)\Omega_y}{\Omega_x+(1+K)\Omega_y}$; and (4.40d) is obtained based on the definition of the Marcum Q-function.

The outage probability can be evaluated based on [78, Eq. 42], as given by

$$\begin{aligned} P'_{\text{out}} &= \Pr\left(Z \le \sigma^2\rho_{\text{th}}\right) = 1 - \int_{\sigma^2\rho_{\text{th}}}^\infty f_Z(z)dz \\ &= 1 - \int_{\sigma^2\rho_{\text{th}}}^\infty \frac{B\exp\left(-K+\frac{B}{2}+\frac{z}{\Omega_y}\right)}{2K\Omega_y} Q\left(\sqrt{B}, \sqrt{Az}\right) dz \\ &= \underbrace{1 - Q\left(\sqrt{2K}, \sqrt{\frac{2(1+K)\sigma^2\rho_{\text{th}}}{\Omega_x}}\right)}_{P_{\text{out}}} + \underbrace{\frac{B}{2K}\exp\left(-K+\frac{B}{2}+\frac{\sigma^2\rho_{\text{th}}}{\Omega_y}\right) Q\left(\sqrt{B}, \sqrt{A\sigma^2\rho_{\text{th}}}\right)}_{\Delta P}. \end{aligned} \tag{4.41}$$

Let $\Omega_m = \frac{(1+K)\Omega_y}{\Omega_x+(1+K)\Omega_y}$, $0 < \Omega_m < 1$. We have $A = \frac{2(1+K)}{\Omega_x\Omega_m}$ and $B = 2K\Omega_m$. ΔP

can be further rewritten as

$$\Delta P = \Omega_m \exp\left(-K + K\Omega_m + \frac{\sigma^2\rho_{\text{th}}}{\Omega_y}\right) Q\left(\sqrt{2K\Omega_m}, \sqrt{\frac{2(1+K)\sigma^2\rho_{\text{th}}}{\Omega_x\Omega_m}}\right). \tag{4.42}$$

Based on the strict monotonicity of the generalized Marcum-Q function [79], we can obtain

$$Q\left(\sqrt{2K\Omega_m}, \sqrt{\frac{2(1+K)\sigma^2\rho_{\text{th}}}{\Omega_x\Omega_m}}\right) \leq Q\left(\sqrt{2K}, \sqrt{\frac{2(1+K)\sigma^2\rho_{\text{th}}}{\Omega_x\Omega_m}}\right) \tag{4.43a}$$

$$\approx \exp\left[-e^{\nu\left(\sqrt{2K}\right)}\left(\frac{2(1+K)\sigma^2\rho_{\text{th}}}{\Omega_x\Omega_m}\right)^{\frac{1}{2}\mu\left(\sqrt{2K}\right)}\right], \tag{4.43b}$$

where (4.43a) is due to the fact that, for $b > 0$, $Q(\sqrt{a}, \sqrt{b})$ strictly increases with $a \in [0, \infty)$, i.e., $Q(\sqrt{a_1 + a_2}, \sqrt{b}) > Q(\sqrt{a_1}, \sqrt{b})$ for all $a_1 \geq 0$, $a_2 > 0$ and $b > 0$ [79]; and (4.43b) is obtained by substituting (4.2) into (4.43).

Since $\Omega_x \geq 0$, then $\Omega_m \leq 1$ and $2K\Omega_m \leq 2K$ always hold for any $\alpha_I \geq \alpha$. By substituting (4.43) into (4.41), the upper bound of P'_{out} can be obtained as

$$P'_{\text{out}} \leq P_{\text{out}} + \Omega_m \exp\left(-K + K\Omega_m + \frac{\sigma^2\rho_{\text{th}}}{\Omega_y}\right) \exp\left[-e^{\nu\left(\sqrt{2K}\right)}\left(\frac{2(1+K)\sigma^2\rho_{\text{th}}}{\Omega_x\Omega_m}\right)^{\frac{1}{2}\mu\left(\sqrt{2K}\right)}\right]$$

$$\triangleq \Phi\left(l, l_I\right). \tag{4.44}$$

This concludes the proof.

4.7.5 Proof of Corollary 3.

In the case that $K = 0$, $\nu(\sqrt{2K}) = -\ln 2$ and $\mu(\sqrt{2K}) = 2$. By substituting these into (4.44), we have

$$P'_{\text{out}} \leq P_{\text{out}} + \frac{\Omega_y}{\Omega_x + \Omega_y} \times \exp\left(-\frac{\sigma^2 \rho_{\text{th}}}{\Omega_x}\right) \tag{4.45a}$$

$$\approx 1 - \frac{\Omega_x}{\Omega_x + \Omega_y} \exp\left(-\frac{\sigma^2 \rho_{\text{th}}}{\Omega_x}\right) \triangleq \Psi\left(\Omega_x, \Omega_y\right). \tag{4.45b}$$

Here, (4.45b) can be rewritten as $\mathcal{H}\left(\omega_x, \omega_y\right) = 1 - \frac{\omega_y}{\omega_x + \omega_y} \exp\left(-\sigma^2 \rho_{\text{th}} \omega_x\right)$ by defining $\omega_x = \frac{1}{\Omega_x}$ and $\omega_y = \frac{1}{\Omega_y}$, hence $\mathcal{H}\left(\omega_x, \omega_y\right) = \Psi\left(\Omega_x, \Omega_y\right)$. By substituting $\Omega_x = P l^{-\alpha}$ and $\Omega_y = P_I \rho_{\text{th}} l_I^{-\alpha_I}$ into $\Psi\left(\Omega_x, \Omega_y\right)$, we can write the outage probability as a function of l/l_I, denoted by $\Phi_0\left(l, l_I\right)$.

We find that

$$\frac{\partial \mathcal{H}\left(\omega_x, \omega_y\right)}{\partial \omega_x} = \left[\frac{\omega_y}{\left(\omega_x + \omega_y\right)^2} + \frac{\omega_y \sigma^2 \rho_{\text{th}}}{\omega_x + \omega_y}\right] \exp\left(-\sigma^2 \rho_{\text{th}} \omega_x\right) \geq 0,$$

and

$$\frac{\partial^2 \mathcal{H}\left(\omega_x, \omega_y\right)}{\partial {\omega_x}^2} = \exp\left(-\sigma^2 \rho_{\text{th}} \omega_x\right) \left[-\frac{2\omega_y}{\left(\omega_x + \omega_y\right)^3} - \frac{\omega_y \sigma^2 \rho_{\text{th}}}{\left(\omega_x + \omega_y\right)^2} - \sigma^2 \rho_{\text{th}} \left(\frac{\omega_y}{\left(\omega_x + \omega_y\right)^2} + \frac{\omega_y \sigma^2 \rho_{\text{th}}}{\omega_x + \omega_y}\right)\right] \leq 0.$$

Thus, $\mathcal{H}\left(\cdot\right)$ is concave with respect to ω_x.

In high SNR regimes (i.e., $\sigma^2 \rho_{\text{th}} \ll \Omega_x \ll 1$), we have

$$\frac{\partial \Psi\left(\Omega_x, \Omega_y\right)}{\partial \Omega_x} = -\left(\frac{\Omega_y}{\left(\Omega_x + \Omega_y\right)^2} + \frac{\sigma^2 \rho_{\text{th}}}{\Omega_x \left(\Omega_x + \Omega_y\right)}\right) \exp\left(-\frac{\sigma^2 \rho_{\text{th}}}{\Omega_x}\right) \leq 0,$$

and

$$\frac{\partial^2 \Psi\left(\Omega_x, \Omega_y\right)}{\partial {\Omega_x}^2} = \left[\frac{2\Omega_y}{\left(\Omega_x+\Omega_y\right)^3} + \frac{\sigma^2\rho_{\text{th}}\left(2\Omega_x+\Omega_y\right)}{{\Omega_x}^2\left(\Omega_x+\Omega_y\right)^2} - \frac{\sigma^2\rho_{\text{th}}}{{\Omega_x}^2}\left(\frac{\Omega_y}{\left(\Omega_x+\Omega_y\right)^2} + \frac{\sigma^2\rho_{\text{th}}}{\Omega_x\left(\Omega_x+\Omega_y\right)}\right)\right] \times \exp\left(-\frac{\sigma^2\rho_{\text{th}}}{\Omega_x}\right),$$

where $\frac{\partial^2 \Psi(\Omega_x,\Omega_y)}{\partial {\Omega_x}^2} \geq 0$*. Thus, $\Psi\left(\cdot\right)$ is convex with respect to Ω_x in high SNR regimes.

Based on the Jensen's inequality (i.e., $\mathbb{E}\left[f(x)\right] \geq f\left(\mathbb{E}\left[x\right]\right)$ if $f(x)$ is convex [80]), the convexity of $\Psi\left(\Omega_x, \Omega_y\right)$ with respect to Ω_x and the concavity of $\mathcal{H}\left(\omega_x, \omega_y\right)$ with respect to ω_x, we have

$$\mathbb{E}\left[\Psi\left(\Omega_x, \Omega_y\right)\right] \geq \Psi\left(\mathbb{E}\left[\Omega_x\right], \Omega_y\right),$$

$$\mathbb{E}\left[\mathcal{H}\left(\omega_x, \omega_y\right)\right] \leq \mathcal{H}\left(\mathbb{E}\left[\omega_x\right], \omega_y\right).$$

Since $\mathcal{H}\left(\omega_x, \omega_y\right) = \Psi\left(\Omega_x, \Omega_y\right)$, we have

$$\Psi\left(\mathbb{E}\left[\Omega_x\right], \Omega_y\right) \leq \mathbb{E}_{\Omega_x}\left[\Psi\left(\Omega_x, \Omega_y\right)\right] = \mathbb{E}_l\left[\Phi_0\left(l, l_I\right)\right] = \mathbb{E}_{\omega_x}\left[\mathcal{H}\left(\omega_x, \omega_y\right)\right] \leq \mathcal{H}\left(\mathbb{E}\left[\omega_x\right], \omega_y\right). \tag{4.46}$$

Since $\Omega_x = Pl^{-\alpha}$, we have

$$\mathbb{E}\left[\Omega_x\right] = \mathbb{E}\left[Pl^{-\alpha}\right] \geq P\left(\mathbb{E}\left[l\right]\right)^{-\alpha}, \tag{4.47}$$

$$\mathbb{E}\left[\omega_x\right] = \mathbb{E}\left[\frac{l^\alpha}{P}\right] \geq \frac{1}{P}\left(\mathbb{E}\left[l\right]\right)^{\alpha}. \tag{4.48}$$

Since $\frac{\partial \mathcal{H}(\omega_x,\omega_y)}{\partial \omega_x} \geq 0$ (given ω_y) and $\frac{\partial \Psi(\Omega_x,\Omega_y)}{\partial \Omega_x} \leq 0$ (given Ω_y), $\mathcal{H}\left(\omega_x, \omega_y\right)$ and $\Psi\left(\Omega_x, \Omega_y\right)$ are monotonically increasing and decreasing functions of ω_x and Ω_x, respectively.

* $\frac{\partial^2 \Psi(\Omega_x)}{\partial {\Omega_x}^2} \geq 0$ holds under the condition that $\sigma^2\rho_{\text{th}} \ll \Omega_x \ll 1$. This condition is typically valid, as Ω_x and $\sigma^2\rho_{\text{th}}$ correspond to the signal power and the noise power at the aerial receiver, respectively.

Therefore, we have

$$\Phi_0\left(\mathbb{E}\left[l\right], l_I\right) = \mathcal{H}\left(\frac{\left(\mathbb{E}\left[l\right]\right)^{\alpha}}{P}, \omega_y\right) \leq \mathcal{H}\left(\mathbb{E}\left[\omega_x\right], \omega_y\right), \tag{4.49}$$

$$\Psi\left(\mathbb{E}\left[\Omega_x\right], \Omega_y\right) \leq \Psi\left(P\left(\mathbb{E}\left[l\right]\right)^{-\alpha}, \Omega_y\right) = \Phi_0\left(\mathbb{E}\left[l\right], l_I\right). \tag{4.50}$$

Comparing (4.46), (4.49) and (4.50), we find that $\Phi_0\left(\mathbb{E}\left[l\right], l_I\right)$ lies between the lower and upper bounds of $\mathbb{E}_l\left[\Phi_0\left(l, l_I\right)\right]$ and we can approximate

$$\mathbb{E}_l\left[\Phi_0\left(l, l_I\right)\right] \approx \Phi_0\left(\mathbb{E}\left[l\right], l_I\right), \tag{4.51}$$

since $\mathcal{X} - \mathbb{E}\left[\mathcal{X}\right] \xrightarrow{a.s.} 0$ with the proof provided in Appendix 4.7.3.

Likewise, we have $\frac{\partial \mathcal{H}(\omega_x, \omega_y)}{\partial \omega_y} \leq 0$ and $\frac{\partial^2 \mathcal{H}(\omega_x, \omega_y)}{\partial {\omega_y}^2} \geq 0$. Thus, $\mathcal{H}\left(\omega_x, \omega_y\right)$ is convex with respect to ω_y. Besides, $\frac{\partial \Psi(\Omega_x, \Omega_y)}{\partial \Omega_y} \geq 0$ and $\frac{\partial^2 \Psi(\Omega_x, \Omega_y)}{\partial {\Omega_y}^2} \leq 0$. Thus, $\Psi\left(\Omega_x, \Omega_y\right)$ is concave with respect to Ω_y. Based on the Jensen's inequality, we have

$$\Psi\left(\Omega_x, \mathbb{E}\left[\Omega_y\right]\right) \geq \mathbb{E}_{\Omega_y}\left[\Psi\left(\Omega_x, \Omega_y\right)\right] = \mathbb{E}_{l_I}\left[\Phi_0\left(l, l_I\right)\right] = \mathbb{E}_{\omega_y}\left[\mathcal{H}\left(\omega_x, \omega_y\right)\right] \geq \mathcal{H}\left(\omega_x, \mathbb{E}\left[\omega_y\right]\right). \tag{4.52}$$

Since $\Omega_y = P_I {l_I}^{-\alpha_I} \rho_{\text{th}}$, we have

$$\mathbb{E}\left[\Omega_y\right] = \mathbb{E}\left[P_I \rho_{\text{th}} l^{-\alpha_I}\right] \geq P_I \rho_{\text{th}} \left(\mathbb{E}\left[l_I\right]\right)^{-\alpha_I}, \tag{4.53}$$

$$\mathbb{E}\left[\omega_y\right] = \mathbb{E}\left[\frac{l_I^{\alpha_I}}{P_I \rho_{\text{th}}}\right] \geq \frac{1}{P_I \rho_{\text{th}}} \left(\mathbb{E}\left[l_I\right]\right)^{\alpha_I}. \tag{4.54}$$

Since $\frac{\partial \mathcal{H}(\omega_x, \omega_y)}{\partial \omega_y} \leq 0$ (given ω_x) and $\frac{\partial \Psi(\Omega_x, \Omega_y)}{\partial \Omega_y} \leq 0$ (given Ω_x), $\mathcal{H}\left(\omega_x, \omega_y\right)$ and $\Psi\left(\Omega_x, \Omega_y\right)$ are monotonically decreasing and increasing functions of ω_y and Ω_y, respectively. Therefore, we have

$$\Phi_0\left(l, \mathbb{E}\left[l_I\right]\right) = \mathcal{H}\left(\omega_x, \frac{1}{P_I \rho_{\text{th}}} \left(\mathbb{E}\left[l_I\right]\right)^{\alpha_I}\right) \geq \mathcal{H}\left(\mathbb{E}\left[\omega_x\right], \omega_y\right), \tag{4.55}$$

$$\Psi\left(\Omega_x, \mathbb{E}\left[\Omega_y\right]\right) \geq \Psi\left(\Omega_x, P_I \rho_{\text{th}} \left(\mathbb{E}\left[l_I\right]\right)^{-\alpha_I}\right) = \Phi_0\left(l, \mathbb{E}\left[l_I\right]\right). \tag{4.56}$$

Comparing (4.52), (4.55) and (4.56), we find that $\Phi_0\left(l, \mathbb{E}\left[l_I\right]\right)$ lies between the lower and upper bounds of $\mathbb{E}_{l_I}\left[\Phi_0\left(l, l_I\right)\right]$, and therefore

$$\mathbb{E}_{l_I}\left[\Phi_0\left(l, l_I\right)\right] \approx \Phi_0\left(l, \mathbb{E}\left[l_I\right]\right), \tag{4.57}$$

since $\mathcal{X} - \mathbb{E}\left[\mathcal{X}\right] \xrightarrow{a.s.} 0$.

Combining (4.51) and (4.57), we have

$$\mathbb{E}_{l,l_I}\left[\Phi_0\left(l, l_I\right)\right] \approx \Phi_0\left(\mathbb{E}\left[l\right], \mathbb{E}\left[l_I\right]\right). \tag{4.58}$$

This concludes the proof.

Chapter 5

Secure Connectivity Analysis of UAV-enabled Wireless Networks

5.1 Introduction

UAVs can be used as relays or aerial base stations for network provisioning in an emergency due to their easy deployment and wide coverage [10]. When the task is complicated, such as providing temporary communication for an earthquake area, a single UAV is usually insufficient. Besides, due to their typically low transmission power and limited processing ability, UAVs usually have only limited transmission range. As such, UAVs are generally organized in an ad hoc manner, forming UAV Networks, and multi-hop relays are adopted for long-distance transmission. Thus, it is essential to study how the connectivity varies among nodes in UAV Networks and evaluate the successful delivery of gathered information in terms of probability.

Consider a search and rescue scenario after an earthquake; several key issues need to be addressed, including victims rescue and environment exploration. UAV Networks can be established for temporary communication between rescuers and disaster victims, or for exploring the terrain and environment information to facilitate the subsequent search and rescue. Disaster areas are more likely to experience power interruption, so some types of UAVs (such as quadrotors) frequently need to operate on battery power, and UAV networks must meet energy efficiency challenges [81]. Meanwhile, security is also essential for UAV Networks. Nodes in UAV Networks are prone to power failure and equipment damage, which may cause errors in information delivery. Worse still, hostile nodes may try to intercept the information

transfer between legitimate nodes or act in malicious ways to prevent UAVs from proper functioning.

Many researchers have developed trust models to evaluate the trust relationships among nodes in MANETs [82, 83]. A detailed survey on various trust models that are geared toward WSNs is presented in [84], which also analyzes various applications of trust models. In [83], a unified trust management scheme using uncertain reasoning is proposed, which consists of two components: trust from direct observation and indirect observation. The trust from direct observation is derived using Bayesian inference, whereas the trust from indirect observation is derived using the Dempster-Shafer theory. An Efficient Distributed Trust Model (EDTM) for WSNs is proposed in [85], and direct trust and recommendation trust are selectively calculated according to the number of packets received by sensor nodes.

However, these trust models are mainly based on communication behaviors, and important factors such as a node's residual energy, the channel between nodes and the mobility pattern of the nodes are not considered. An information-theoretic framework is presented in [86], and the trust model takes the dynamic behaviors of nodes and the wireless environment into consideration. Moreover, a fuzzy-logic based prediction mechanism is adopted to update a node's trust for future decision-making. In [87], an attack-resistant trust model based on multidimensional trust metrics (ARTMM) is proposed for underwater acoustic sensor networks (UASNs), which consists of three types of trust metrics, i.e., link trust, data trust, and node trust. It also takes the slow-movement of underwater sensor nodes into consideration. However, these trust models may not function well in UAV Networks, because of their highly dynamic network topology, the high mobility of UAVs, and the open-air wireless environment. Due to this dynamic topology, the trust relationships between UAVs are frequently changed in UAV Networks. Trust is a dynamic process and changes with time and the surrounding environment, but most existing

trust models do not address the dynamic issues. In order to solve the above problems, we propose a novel trust model that can evaluate the trust levels between UAVs by considering multiple practical factors and their highly dynamic nature.

In this chapter, trust is defined as the degree of belief (probability) that a UAV will execute a task correctly according to the previous observation of its behavior. That is, the trust value reflects whether a given UAV behaves in a trustworthy manner and maintains reliable communications with other nodes in UAV Networks. A trust value is a number in the range of 0 to 1. A value of 1 means completely trustworthy, and 0 means completely untrustworthy.

The contributions of this chapter are outlined as follows.

- We propose an EHTM that takes into consideration the UAVs' behaviors, the characteristics of channels between UAVs and the mobility of UAVs. The detailed calculation procedure of EHTM is also presented.

- We propose the concept of secure links in UAV Networks. A secure link exists between two UAVs only when there is both a physical link and a trust link between them. The physical link indicates physical connectivity between two UAVs, which means each UAV on a routing path is within the communication range of its previous UAV. Based on the proposed trust model, the trust link between two UAVs can be viewed as a logical connectivity between these two nodes. One simple parameter, the trust value or belief degree, $\mathbf{P}_{\mathrm{T}}$, is introduced to quantify the trustworthiness of the trust link between two nodes.

- We derive both the physical connectivity probability and the secure connectivity probability between two UAVs in the presence of Doppler shift. The proposed trust model, physical connectivity and secure connectivity probability in the UAV Networks are evaluated by simulation. Extensive simulation results show that the proposed trust model can effectively guarantee secure and reli-

able communication between UAVs and enhance the connectivity probability when the UAV Networks suffer attacks and other security risks.

The rest of this chapter is organized as follows. In Section 5.2, we introduce the system model. The trust model and the detailed trust calculation procedure of EHTM is presented is presented in Section 5.3. Section 5.4 analyses the secure connectivity probability between UAVs and simulation results and analysis are presented in Section 5.5. Finally, Section 5.6 concludes the chapter.

5.2 System Model and Definitions

In this section, we first present the network model, mainly considering the search and rescue scenario. Then, we describe the basic mobility model for UAVs. Finally, we give a brief definition of the secure link in UAV Networks.

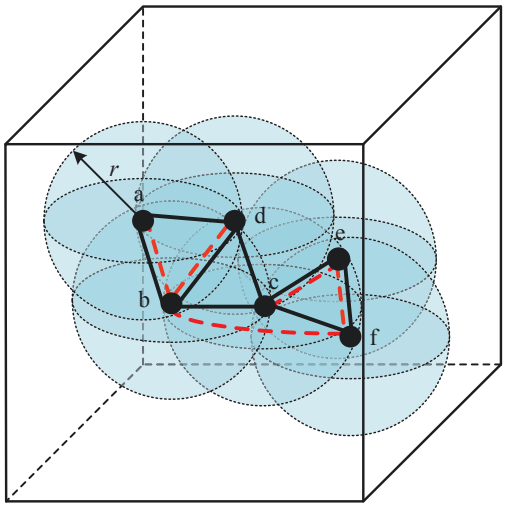


Figure 5.1 : An illustration of a UAV network with a trust link. Here, solid lines and dotted lines denote physical links and trust links, respectively.

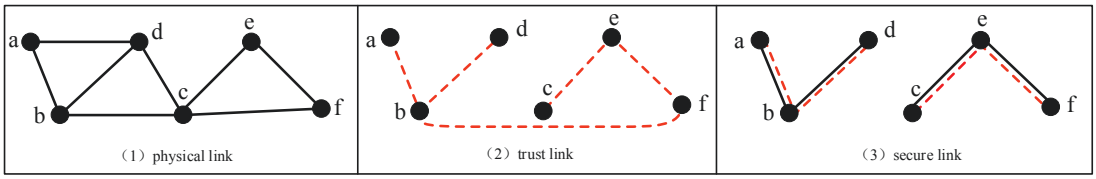


Figure 5.2 : Secure link abstracted from UAV Networks in Fig. 5.1. (1) physical link; (b) trust link; (c) secure link.

5.2.1 Network Model

We consider a UAV network, in which UAVs are deployed in an infinite 3D Euclidean space according to a homogeneous Poisson point process (PPP) with density λ, as depicted in Fig. 5.1. The UAVs have a maximum one-hop communication range, which is denoted by r. A UAV can transmit information to the intended destination directly, or via indirect relay by one or more UAVs. The multi-hop scheme is decode-and-forward, in which the relaying UAV decodes an arriving packet and then transmits to the next hop.

We adopt the ST mobility model [59, 60] to model the motion of UAVs. ST captures the tendency of UAVs to make smooth trajectories (e.g., straight trajectories or typical turns with a large radius) and is widely used in UAV networks analysis. The ST mobility model captures the correlation of acceleration of UAVs across the temporal and spatial domain and is tractable for analysis and design. Wan et. al. prove that the stationary node distribution of the ST model is uniform [60], which leads to a series of closed-form results for connectivity.

5.2.2 Definition of Secure Links

5.2.2.1 Physical Link.

Two UAVs, N_i and N_j have a physical wireless link if their Euclidean distance is no greater than the communication range r, and N_i and N_j are called *physical*

neighbors. Two UAVs are physically connected if there is a physical path from the source node to the destination node and each node on the path lies in the communication range of its previous node.

5.2.2.2 Trust Link.

A trust link can be viewed as a logical connection between two UAVs in UAV Networks. One simple parameter, the trust value or belief degree, $\mathbf{P}_{\mathrm{T}}$, is introduced to quantify the existence of trust link between two UAVs in the UAV Networks. If $\mathbf{P}_{\mathrm{T}}$ is greater than or equal to 0.5, the trust link is considered to exist. Otherwise, it does not exist. We call two UAVs with a trust link, *friends*.

5.2.2.3 Secure Link.

A secure link exists between two UAVs only when there is both a physical link and a trust link between these two nodes. This means that each UAV not only has neighbor nodes within its communication range, but also can establish trust links with these neighbor nodes. We call N_i the *neighboring friend* of N_j if a secure physical link exists between N_i and N_j.

5.3 Trust Modeling and Calculation

In this section, we propose an EHTM. To compute the trust value of UAVs, it is important to understand the trust definition and properties that are used in the trust calculation. Then, we describe the overall structure of the EHTM.

5.3.1 Efficient Hierarchical Trust Model

As illustrated in Fig. 5.3, the trust model is composed of four sections: direct trust section, indirect trust section, integrated trust section, and trust update section.

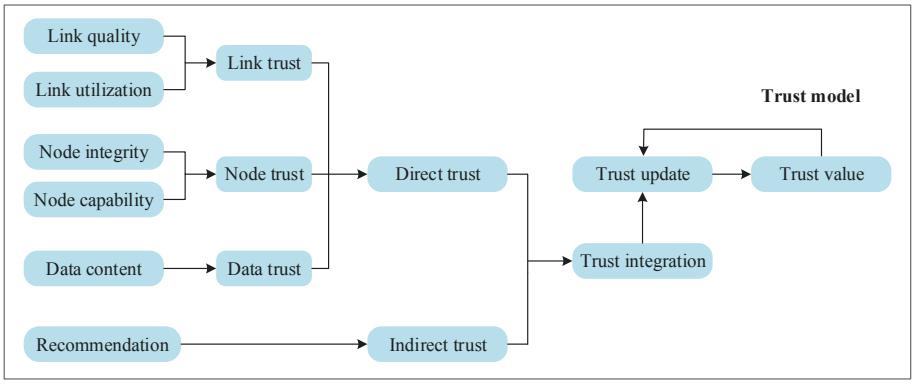


Figure 5.3 : The structure of trust model

In a direct trust model, the trust value is computed based on the communication behaviors of UAVs, the channels between UAVs, and the mobility of UAVs. However, due to malicious attacks, adopting only direct trust is not sufficient. In addition, it is difficult to decide whether a UAV is benign or malicious based on only a few interactions when the number of packet exchanges between two UAVs is small. Therefore, packet threshold is defined and denoted as ζ_{th}. If the number of packet exchanges between a pair of nodes exceeds the threshold ζ_{th}, the trust value is only calculated by the direct trust. Otherwise, assessments from other node are required for trust estimation. In this case, we need to calculate both the direct and indirect trust and then combine them by using a weighted average to obtain the integrated trust.

In UAV Networks, UAVs collaborate to transmit information through communication channels. In a natural disaster, UAVs can be easily attacked or launch many kinds of malicious attacks, e.g., packet modification attacks and packet dropping attacks, which can result in low link quality. In addition, the communication channel between UAVs is unreliable, which may introduce a high packet error rate (PER) and packet loss rate (PLR). The communication performance and data transmission are affected by the quality of the channel. Therefore, the trust value is not only

related to the participating UAVs but also impaired by the link quality.

As shown in Fig. 5.3, the direct trust module consists of three components: link trust, node trust, and data trust. Link trust is evaluated by link quality and link utilization. Link quality illustrates the performance of the communication channel between UAVs, which is calculated based on the PER and PLR estimations of the link. Link utilization is defined as the ratio of the number of times a link is utilized over the maximum possible number of times it can be used. Data trust reflects the trustworthiness of data content transmitted between UAVs, which can be assessed by the fault tolerance and consistency of data. Node trust is determined by node integrity and node capability. Node integrity indicates the degree to which one UAV believes its neighbor node is honest based on their communication behaviors (successful and failure communications). Node capability refers to whether the residual energy in one UAV is adequate to perform the desired task. Therefore, it is computed according to the energy consumption of UAVs. According to the link trust, the node trust and the data trust, we can obtain direct trust by the weighted average method. In addition, the indirect can be calculated from the third-party recommendation. Finally, the trust value can be achieved through the trust integration section and the trust update section.

5.3.2 Trust Calculation

In this section, we present the detailed EHTM trust calculation procedure.

5.3.2.1 Calculation of Direct Trust

Direct trust in this chapter takes link trust, data trust and node trust into consideration.

(1) Link Trust

Link trust is determined by link quality and link utilization in this chapter.

Calculation of the PER. We chose the Rician fading model for the UAV channel, due to the existence of an LoS path between UAVs in an open-air scenario. The average bit error rate (BER) for two-phase differential phase shift keying (2DPSK) modulation under the Rician fading channel is given in [88] as

$$P_{\text{ber}} = \frac{1}{2}\left(\frac{1+K}{1+K+\bar{\gamma}}\right)\exp\left(-\frac{K\bar{\gamma}}{1+K+\bar{\gamma}}\right), \tag{5.1}$$

where K is the Rician factor, and $\bar{\gamma}$ is the average (SNR), $\bar{\gamma} = \frac{P_0}{{\sigma_N}^2 d^2}$ (P_0 is the transmitting power, ${\sigma_N}^2$ is the noise power and d is the distance between the source UAV and the destination UAV). In the next step, we compute the PER based on the BER. The probability of not having a bit error is equal to the probability that all the bits are received correctly. Thus the PER is calculated as follows:

$$P_{\text{per}} = 1 - (1 - P_{\text{ber}})^n, \tag{5.2}$$

where n denotes the number of bits in a packet.

Calculation of the PLR. There are several metrics for link quality in UAV Networks, such as the received signal strength indicator (RSSI), packet receiving ratio (PRR), and link quality indicator (LQI). In this chapter, we chose the PRR for the link quality evaluation. The PRR is usually calculated by the destination node and expressed as $P_{\text{prr}} = p_{rec}/p_{\text{sen}}$, where p_{rec} and p_{sen} denote the number of successfully received packets in the object UAV node and the total packets sent from subject node respectively.

Then, the packet loss rate can be calculated by by $P_{\text{loss}} = 1 - P_{\text{prr}}$. According

to Equations (3) and (4), the link quality $\mathbf{L}_{lq}$ can be computed by

$$\mathbf{L}_{\text{lq}} = (1 - P_{\text{per}}) \times (1 - P_{\text{loss}}) = (1 - P_{\text{per}}) \cdot P_{\text{prr}}. \tag{5.3}$$

Calculation of Link Utilization. Link utilization, $\mathbf{L}_{\text{lu}}$, is defined as the ratio of the number of times a link is utilized over the maximum possible number of times it can be used. According to the routing table entry of UAVs, the maximum possible number of utilization times can be obtained.

$$\mathbf{L}_{\text{lu}} = \frac{N_{\text{use}}}{N_{\text{max}}}, \tag{5.4}$$

where N_{use} is the number of times a link is utilized in the current time window and N_{max} is the maximum possible number of times that the link can be used.

We define 0.5 as the chosen trust threshold. The link trust depends on the link quality and link utilization. If the link is of poor quality, $\mathbf{L}_{\text{lq}} < 0.5$, the link is considered as untrustworthy even if the link utilization is high. Therefore, when $\mathbf{L}_{\text{lq}} < 0.5$, the link trust is defined as $\mathbf{L}_{\text{lq}} \times \mathbf{L}_{\text{lu}}$. However, the definition is not suitable when $\mathbf{L}_{\text{lq}} > 0.5$. For example, if $\mathbf{L}_{\text{lq}} = 0.8$ and $\mathbf{L}_{\text{lu}} = 0.6$, the link trust is 0.48. In this case, the link should be trustworthy even though its calculated trust value is less than 0.5. Therefore, the link trust is redefined as $0.5 + (\mathbf{L}_{\text{lq}} - 0.5) \times \mathbf{L}_{\text{lu}}$. Then the link trust can be obtained as:

$$\mathbf{T}_{\text{link}} = \begin{cases} 0.5 + (\mathbf{L}_{\text{lq}} - 0.5) \times \mathbf{L}_{\text{lu}}, & \text{if } \mathbf{L}_{\text{lq}} \geq 0.5; \\ \mathbf{L}_{\text{lq}} \times \mathbf{L}_{\text{lu}}, & \text{else.} \end{cases} \tag{5.5}$$

(2) Node Trust

Node trust is computed by considering both node integrity and node capability. Node integrity is evaluated based on the direct communication behaviors of one UAV to check whether the node is reliable or not.

Node Integrity. In UAV Networks, UAVs move rapidly, the network topology changes dynamically, and the communication links between UAVs are unstable. Thus UAV communication behaviors in UAV Networks involves considerable uncertainty. To deal with this uncertainty, we adopt a Subjective Logic framework [89]. The trust value in the Subjective Logic framework is denoted by a triplet $T = \{b, d, u\}$, where b, d and u correspond to belief, disbelief, and uncertainty, respectively, $b, d, u \in [0, 1]$, $b + d + u = 1$. On the basis of a Subjective Logic framework, the trust model for node integrity is established, and node integrity $\mathbf{N}_{\text{ni}}$ can be calculated by:

$$\mathbf{N}_{\text{ni}} = \frac{2b + u}{2}, \tag{5.6}$$

where $b = \frac{s}{s+f+1}$ and $u = \frac{1}{s+f+1}$. s and f are the number of successful and unsuccessful communications between UAVs in UAV Networks. Successful or failure communication between two nodes depends on the link quality (packet loss ratio), thus the number of successful and failed communications between UAVs can be adjusted as:

$$s' = s + P_{\text{loss}} \times (s + f), \tag{5.7}$$

$$f' = f - P_{\text{loss}} \times (s + f). \tag{5.8}$$

Node Capability. Node capability is the assessment of the residual energy level of UAVs. It is assumed that the initial energy set and energy consumption rate of all UAVs are the same in UAV Networks. However, when malicious UAVs launch malicious attacks in UAV Networks, the energy consumed by them is abnormal.

Normal nodes consume less energy than malicious nodes. Therefore, we determine whether the node is malicious or not according to its energy consumption. First, we define an energy consumption threshold E_{th}. When the residual energy of the UAV is below the threshold, the node cannot accomplish the expected task. In this case, node capability is assumed to be zero. Otherwise, node capability can be computed by the energy consumption rate r_{ene}, $r_{\text{ene}} \in [0, 1]$. The higher the energy consumption rate is, the less residual energy remains, which leads to weaker node capability. Thus, node capability $\mathbf{N}_{\text{nc}}$ is expressed as:

$$\mathbf{N}_{\text{nc}} = (1 - r_{\text{ene}}) \times \mathbf{1}\left(E_{\text{res}} \geq E_{\text{th}}\right), \tag{5.9}$$

where r_{ene} is calculated by the method introduced in [90], and

$$\mathbf{1}\left(E_{\text{res}} \geq E_{\text{th}}\right) = \begin{cases} 1, & E_{\text{res}} \geq E_{\text{th}}; \\ 0, & E_{\text{res}} < E_{\text{th}}. \end{cases}$$

.

Based on node integrity and node capability, node trust can be evaluated as follows:

$$\mathbf{T}_{\text{node}} = \begin{cases} 0.5 + (\mathbf{N}_{\text{ni}} - 0.5) \times \mathbf{N}_{\text{nc}}, & \text{if } \mathbf{N}_{\text{nc}} \geq 0.5; \\ \mathbf{N}_{\text{ni}} \times \mathbf{N}_{\text{nc}}, & \text{else.} \end{cases} \tag{5.10}$$

(3) Data Trust

Data transmission is subject to several sources of errors such as noise from external sources, hardware noise, inaccuracies and imprecision, and various environmental effects [91]. Such errors may severely impact the trustworthiness of the data. Therefore, data trust evaluation is introduced in this chapter. It assesses the trust value of the fault tolerance and data consistency. Generally, data information has tempo-

ral and spatial correlations; that is, in a specific time period the data sent among neighboring UAVs are always similar in the same area. The numerical value of the data information always follows specific distributions, such as normal distribution and exponential distribution. For simplicity, we assume the distribution of data items complies with a normal distribution and the probability density function is $f(x) = \frac{1}{\sigma\sqrt{2\pi}} \exp\left(-\frac{(x-\mu)^2}{2\sigma^2}\right)$, where x is the attribute value v_d of a data item, and μ and σ^2 are the mean and variance of the data. Based on [92], the trust value of the data item is defined as:

$$\mathbf{T}_{\text{data}} = 2\left(0.5 - \int_{\mu}^{v_d} f(x)\, dx\right) = 2\int_{v_d}^{\infty} f(x)\, dx. \tag{5.11}$$

Based on link trust $\mathbf{T}_{\text{link}}$, node trust $\mathbf{T}_{\text{node}}$, and data trust $\mathbf{T}_{\text{data}}$, we can obtain the direct trust between two neighbouring UAVs as:

$$\mathbf{T}_{\text{direct}} = \omega_{\text{link}}\mathbf{T}_{\text{link}} + \omega_{\text{node}}\mathbf{T}_{\text{node}} + \omega_{\text{data}}\mathbf{T}_{\text{data}}, \tag{5.12}$$

where ω_{link}, ω_{node} and ω_{data} are the weight values of the link trust, node trust and data trust, $\omega_{\text{link}} \in [0,1]$, $\omega_{\text{node}} \in [0,1]$, $\omega_{\text{data}} \in [0,1]$, and $\omega_{\text{link}} + \omega_{\text{node}} + \omega_{\text{data}} = 1$.

5.3.2.2 Calculation of Indirect Trust

The third-party recommendation needs to be considered in indirect trust calculation. However, some recommendations are dishonest, and using these false recommendations may lead to an unreliable trust evaluation. Therefore, it is necessary to identify these false recommendations before the trust calculation. In this chapter, we use recommendation trust to evaluate to what extent the recommendation from other nodes can be trusted. Recommendation trust is evaluated based on both node integrity and the recommendation value of each recommendation node. First, it is assumed that one UAV receives the node integrity from l neighbor UAVs. Then,

weighting factor χ_i of recommendations from each recommendation node is computed based on these node integrities, $\chi_i = \frac{\mathbf{N}_{ni}(i)}{\sum_{k \in R} \mathbf{N}_{\mathrm{ni}}(k)}$, where $\mathbf{N}_{\mathrm{ni}}(i)$ denotes the node integrity of node i and R is the set of recommendation nodes. Finally, the recommendation trust is obtained as:

$$\mathbf{T}_{\mathrm{rec}} = \frac{\sum_{i=1}^{l} \chi_i \times T_i}{l}, \tag{5.13}$$

where T_i is the recommendation value from recommendation node i.

5.3.2.3 Integrated Trust Calculation

When the communication packets between the subject UAVs and object UAVs are higher than the threshold ζ_{th}, the trust value is only calculated by the direct trust. Otherwise, the recommendations from third parties are needed for the trust estimation. Therefore, the trust value can be calculated as:

$$\mathbf{P}_{\mathrm{T}} = \begin{cases} \mathbf{T}_{\mathrm{direct}}, & \text{if } s' \geq \zeta_{\mathrm{th}}; \\ \omega \mathbf{T}_{\mathrm{direct}} + (1-\omega)\,\mathbf{T}_{\mathrm{rec}}, & \text{otherwise.} \end{cases} \tag{5.14}$$

where ω is the weight value for the direct trust.

5.3.2.4 Trust Update

Due to the highly dynamic nature of the UAV networks, UAVs enter and leave the network rapidly, so the trust value needs to be updated periodically. The length of the update interval will affect network performance. If the update interval is too long, it cannot adequately reflect the current behavior of the object UAV. If the update time is too short, it may consume too much energy. Therefore, the concept of a sliding time window is adopted to update the trust value.

A time window consists of several time slots. During each time window, the

current trust value of the object UAV can be calculated. Then, in the next time window, the historical trust values can be used to update the new trust value. As we all know, time decay is an important property of the trust, which means that historical behavior is not as important as current behavior. Thus, when using historical trust values to update current values, it is necessary to consider a time decay factor for historical trust values. In [93], the trust value decays exponentially with time, while it decreases linearly with time in [94]. In this chapter, we chose the exponential decay in the trust model, which is defined as:

$$\omega_d = \exp\left(-\delta\left(t_i - t_{i-1}\right)\right), \tag{5.15}$$

where δ is the a regulatory factor, $\delta \in (0, 1)$. t_i and t_{i-1} are the trust calculation time of the current and historical trust values, respectively.

Based on the current trust values $\mathbf{P}_{\mathrm{T}}(i)$ and the historical trust values $\mathbf{P}_{\mathrm{T}}(i-1)$, the trust value can be updated as:

$$\mathbf{P}_{\mathrm{T}}(i)_{new} = \omega_d \mathbf{P}_{\mathrm{T}}(i-1) + (1-\omega_d)\mathbf{P}_{\mathrm{T}}(i). \tag{5.16}$$

5.4 Secure Connectivity Analysis of UAV Networks under Doppler Shifts

In this section, we first analyze the physical connectivity probability between UAVs in UAV Networks using Stochastic Geometry. Then, based on the EHTM, the secure connectivity probability between UAVs is derived.

5.4.1 Physical Connection in UAV Networks

Physical connection in UAV Networks is closely related to the existence of a physical link, which refers to the probability that each node on the path falls within

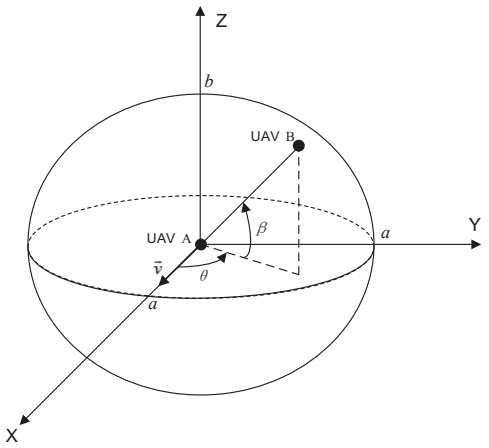


Figure 5.4 : An illustration of the Oblate Spheroid Model

the communication range of its previous node.

5.4.1.1 UAV Isolation Probability

Let M be a random variable denoting the number of UAVs that is present in the communication range of UAV A. Because the UAVs in the UAV networks are uniformly distributed with density λ, it can be shown that M is Poisson distributed with the following probability mass function (PMF):

$$P_M(m) = \frac{\left(\frac{4}{3}\pi r^3\lambda\right)^m}{m!} e^{-\frac{4}{3}\pi r^3\lambda}. \tag{5.17}$$

A UAV will be isolated in the UAV Networks if there is no UAV in its communication range. Let P_i represent the probability that no UAV appears within its communication range; thus the probability of one UAV being isolated is:

$$P_i = P_M(0) = e^{-\frac{4}{3}\pi r^3\lambda}. \tag{5.18}$$

5.4.1.2 UAV Isolation Probability with Doppler Shift

The Doppler effect is the change in frequency of a wave perceived the receiver, due to the relative motion between the transmitter and the receiver. Doppler shift is the value of the frequency change. In most cases, Doppler shift can be eliminated by techniques such as frequency offset estimation in the physical layer. However, if the Doppler frequency offset exceeds a threshold of f_{th}, it is difficult to compensate, and signals quality will be severely affected. The threshold of the Doppler shift is mainly determined by the receiver's hardware. The high mobility of UAVs will cause severe Doppler shift, which will affect the communication quality between UAVs. In a 3D mobile radio environment, the Doppler shift of a signal reaching a UAV receiver is

$$f_d = \frac{v}{c} f_c \cos(\theta) \cos(\beta) = f_m \cos(\theta) \cos(\beta). \tag{5.19}$$

where f_c is the carrier frequency of the signal without Doppler shift, v is the relative moving velocity of the UAV pair, c is the velocity of light, θ and β are the azimuth angle (AA) and elevation angle (EA) of the arriving signal and $f_m = \frac{v}{c} f_c$ is the maximum Doppler shift. For the environment of interest and without loss of generality, we focus on the cases where (i) the AA and EA are random variables that are independent of each other, and (ii) the AA is uniformly distributed in $(-\pi, \pi)$, that is,

$$p_\theta(\theta) = \frac{1}{2\pi}, \quad |\theta| \leq \pi. \tag{5.20}$$

The EA is distributed within $\left(0, \frac{\pi}{2}\right)$, with its probability density function (PDF) denoted by $p_\beta(\beta)$. In order to facilitate the calculation, we define the normalized Doppler shift as $\rho \equiv f_d / f_m = \cos(\theta)\cos(\beta), \quad |\rho| \leq 1$, which implies that $|\gamma| \leq$

$\cos(\theta)$ and $|\gamma| \leq \cos(\beta)$. The cumulative distribution function of ρ is

$$\begin{aligned} F_{\rho}(\rho) &= \Pr\{\cos(\theta)\cos(\beta) \leq \rho\} \\ &= \frac{1}{\pi}\int_{0}^{\pi/2} p_{\beta}(\beta) \left[\int_{\arccos[\rho/\cos(\beta)]}^{\pi} d\theta\right] d\beta. \end{aligned} \tag{5.21}$$

It is difficult to analyze the Doppler shift distribution between two flying UAVs. For analytical tractability, we transform the original problem between two moving UAVs into an equivalent problem between a stationary UAV and a relatively moving UAV. As shown in Fig. 5.4, we chose the receiving UAV as the coordinate origin and the oblate spheroid space surrounding it. If it is assumed that all scatters are uniformly distributed in the space, then the PDF of EA can be obtained according to [95]:

$$p_{\beta}(\beta) = \frac{ab^2\cos(\beta)}{\left(a^2\sin^2(\beta) + b^2\cos^2(\beta)\right)^{3/2}}, \tag{5.22}$$

where a and b are the semi-principle axes along the x and z axes respectively. Defining $\varepsilon \equiv \frac{a}{b}$, we have

$$p_{\beta}(\beta) = \frac{\varepsilon\cos(\beta)}{\left(\varepsilon^2\sin^2(\beta) + \cos^2(\beta)\right)^{3/2}}, \tag{5.23}$$

which is only dependent on the parameter ε. Then we obtain

$$p_{\rho}(\rho) = \frac{\varepsilon}{\pi(\varepsilon^2-1)^{3/2}} H(\rho), \tag{5.24}$$

where

$$H(\rho) = \int_{0}^{\sqrt{1-\rho^2}} \frac{1}{\sqrt{\left[x^2 + 1/(\varepsilon^2-1)\right]^3 (1-\rho^2-x^2)}} dx. \tag{5.25}$$

The integral in (27) can be computed according to *Formula 3.158* provided in [96],

then we can obtain the PDF of the Doppler shift,

$$p_\rho(\rho) = \frac{\varepsilon}{\pi\sqrt{(\varepsilon^2-1)(1-\rho^2)}} E\left(\frac{\sqrt{(\varepsilon^2-1)(1-\rho^2)}}{\sqrt{1+(\varepsilon^2-1)(1-\rho^2)}}\right), \tag{5.26}$$

where $E(k) = \int_0^{\frac{\pi}{2}} \sqrt{1-k^2\sin^2\alpha}\, d\alpha$ is the complete elliptic integral of the second kind, and $k = \frac{\sqrt{(\varepsilon^2-1)(1-\rho^2)}}{\sqrt{1+(\varepsilon^2-1)(1-\rho^2)}}$, $0 \le k \le 1$, is the elliptic eccentricity. When $\rho \to 1$, i.e., $f_d \to f_m$, $k \to 0$ and $E(0) = \frac{\pi}{2}$, we have $p_\rho(\rho) \to \infty$; when $\epsilon \to \infty$, $k \to 1$ and $E(1) = 1$, we have $p_\rho(\rho) \to \frac{1}{\pi}$.

It is assumed that all UAVs in the UAV Networks have the same Doppler shift threshold f_{th}. If the Doppler shift is greater than the threshold, then two UAVs within communication range of each other will not be able to communicate successfully [97]. Therefore, the communication link between two adjacent UAVs is available when two conditions are satisfied at the same time: (1) Two UAVs are within the communication range of each other. (2) The Doppler shift meets the threshold requirement, i.e., $f_d \le f_{\text{th}}$ [97].

According to the PDF of the Doppler shift, we can obtain the probability that the frequency deviation between two UAVs is less than the threshold as:

$$P_{\text{th}} = F_\rho(\rho_{\text{th}}) = \int_0^{\rho_{\text{th}}} p_\rho(\rho)\, d\rho, \tag{5.27}$$

where $\rho_{\text{th}} = f_{\text{th}}/f_m$. The probability that one UAV is not isolated also can be obtained based on the UAV isolation probability. Finally, the physical probability of the available link between two UAVs is calculated as

$$P_{\text{phy}} = (1-P_i)\, P_{\text{th}} = \left(1 - e^{-\frac{4}{3}\pi r^3 \lambda}\right) \cdot F_\rho(\rho_{\text{th}}). \tag{5.28}$$

5.4.2 Secure Connectivity Analysis

In this chapter, we assume the UAVs are distributed in a 3D Euclidean space according to a homogeneous PPP with density λ, so the number of UAVs within the communication range r of the object UAV is $\frac{4}{3}\pi r^3\lambda$. In addition, if the trust value $\mathbf{P}_{\mathrm{T}}$ of the object UAV is taken into consideration, we define the UAV that has trust links to the object node as friends. Then we can acquire the number of neighboring friends that are within the communication range of the object UAV as $\mathbf{P}'_{\mathrm{T}} \cdot \frac{4}{3}\pi r^3\lambda$, where $\mathbf{P}'_{\mathrm{T}} = \frac{1}{M}\sum_{i=1}^{M}\mathbf{P}_{\mathrm{T}i}$, and M is the number of UAVs that are present in the communication range of the object node. Similar to the derivation of the physical probability of the available link between two UAVs, the probability of secure connectivity between two UAVs in the UAV Networks can be obtained as:

$$P_{\mathrm{sec}} = \left(1 - P'_i\right) P_{th} = \left(1 - e^{-\mathcal{P}'_T \cdot \frac{4}{3}\pi r^3\lambda}\right) \cdot F_\rho\left(\rho_{\mathrm{th}}\right), \tag{5.29}$$

where $P'_i = e^{-\mathbf{P}'_{\mathrm{T}} \cdot \frac{4}{3}\pi r^3\lambda}$ is the probability that there are no friends within the communication range of the object UAV.

5.5 Simulation and Evaluation

In this section, the trust model, physical connectivity and secure connectivity probability in the UAV Networks are evaluated by simulation. We implement two different sets of simulations. First, we evaluate the performance of the trust model under various parameters, e.g., different weight values and different trust update time. Then, we compare the physical connectivity probability and secure connectivity probability with or without the trust model on the basis of the performance of the trust model. The deployment area is set to be $10km \times 10km \times 10km$. There are 30 UAVs uniformly deployed in the network area initially, and then they move according to the ST mobility model within the region. Some important parameters

are given in Table 5.1.

Table 5.1 : Simulation parameters [85]

Parameter	Value
Transmit power P_0	5w
Noise power N_0	-20dBm
Rician factor K	10dB
Energy consumption rate r_{ene}	0.4
Residual energy threshold	0.3
Communication packets threshold ζ_{th}	300

5.5.1 Performance of the Trust Model

We first evaluate the trust model between two UAVs. To compare the trust value calculated by the proposed trust model, we first derive objective trust. The objective trust is computed on the basis of each UAV's actual information without taking any malicious attacks into consideration. Then, the malicious UAVs are simulated by a denial-of-service (DoS) attack, and the proportion of malicious UAVs is set as 30 %. As shown in Fig. 5.5 and 5.6, we find that the trust values increase gradually with the simulation time.

Fig. 5.5 illustrates the results of the direct trust value, the integrated trust value and the trust value with the update of UAVs, respectively. We observe that when the communication packets between the subject and the object UAVs are higher than the threshold ζ_{th}, the direct trust is closer to the trust values compared with the integrated trust values because the integrated trust values are influenced by the malicious recommenders. Thus, in this case, we only need to calculate the direct trust values for trust evaluation.

Fig. 5.6 shows that when there are fewer communication packets between the subject and the object UAVs than the threshold ζ_{th}, the integrated trust values are

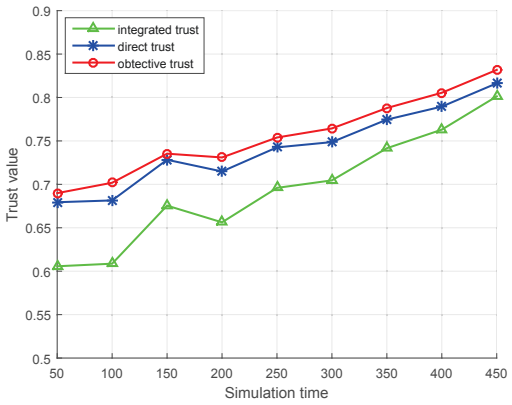


Figure 5.5 : Communication packets are higher than the threshold

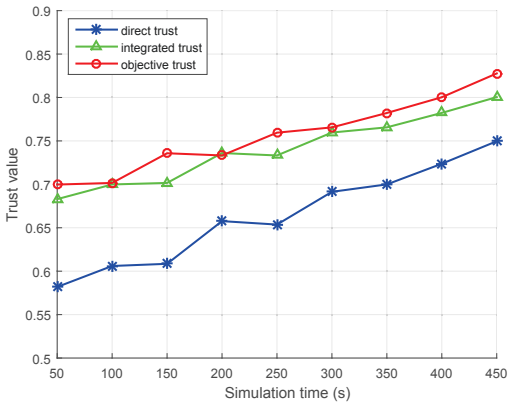


Figure 5.6 : Communication packets are lower than the threshold

closer to the trust values compared with the direct trust values, because there are not enough communication packets between these two UAVs to accurately reflect the actual node behaviors. Therefore, it is essential to take recommendation into consideration for trust evaluation when the number of communication packets is small or the communication time is short.

According to Fig. 5.5 and 5.6, we can conclude that it is important to integrate direct trust and indirect trust when there are not enough packet exchanges for nodes' trust evaluation. In addition, the proper weight values for the direct values and the indirect values change with the environmental conditions. In our trust model, the

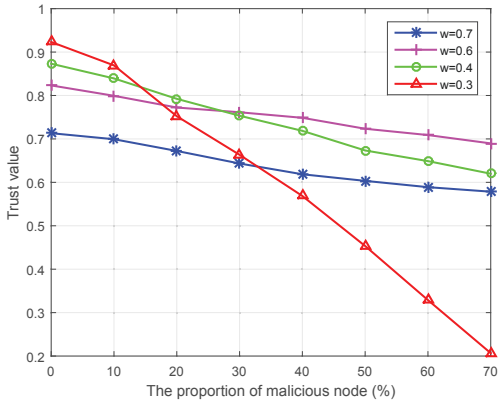


Figure 5.7 : Influence of the weight value

subject UAV adopts the recommendations from neighboring UAVs concerning the object UAV. We assume that the proportion of malicious neighbor UAVs that launch the attack ranges from 0 to 70 % with 10 % increment. It is also assumed that there are enough communication packets between UAVs and that the number of average packets is set at 300 during each period. The weight values for direct trust are denoted as ω.

As shown in Fig. 5.8, the trust value is highest under $\omega = 0.3$ (ω is the weight value for the direct trust) when the percentage of malicious UAVs is less than 10 %. In this case, we only evaluate the trust by calculating the direct trust value because of the small impact of malicious UAVs. In addition, the trust value is higher than 0.5 when the proportion of malicious UAVs is below 45 %. However, as the percentage of malicious UAVs increases continually, the trust value decreases significantly. As the percentage of malicious UAVs in the UAV Networks grows, the weight value of direct trust decreases, and the obtained trust value decreases accordingly. Thus, we can conclude that more malicious nodes in the UAV Networks will result in lower trust values between UAVs. Moreover, the weight values for direct and indirect trust need to be adjusted dynamically according to the number of malicious nodes in the network.

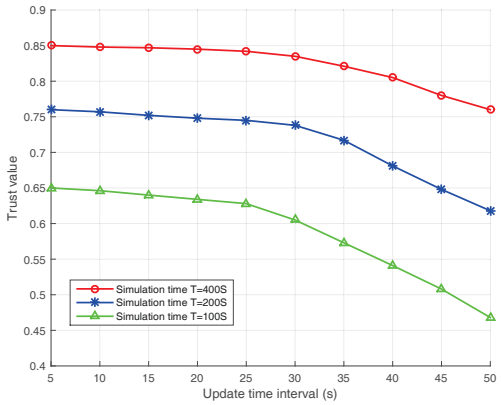


Figure 5.8 : Influence of trust update time interval

In the trust model, the trust values are updated dynamically. Generally, updating the trust value frequently may consume a large amount of energy. Conversely, if the update time interval is too long, it cannot effectively determine the actual behavior of the object UAV. The influence of the trust update time interval on the trust value is evaluated. As shown in Fig. 5.8, the trust value decreases slowly at first and then decreases rapidly with the increased update time interval. Besides, as the simulation time increases, the trust value increases continuously. Thus, to save energy consumption, we can choose a longer time interval for trust evaluation. However, when a more accurate trust value is required, the shorter time interval may be selected.

In Fig. 5.9, the robustness of the proposed trust model is evaluated. We adopt the ST mobility model for UAVs, where the velocity of the UAVs ranges from 50 to 500 m/s. We can see that the proposed trust model can work well in the open-air scenario and be robust against the mobility of UAVs.

5.5.2 Physical Connectivity Probability

In this section, we simulate the physical connectivity probability between two UAVs in the UAV Networks according to the above calculation. We will illustrate

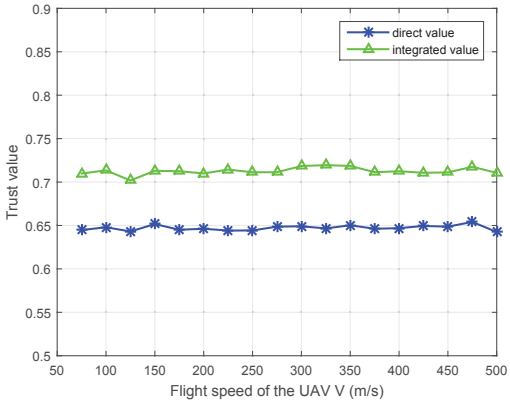


Figure 5.9 : Robustness against mobility

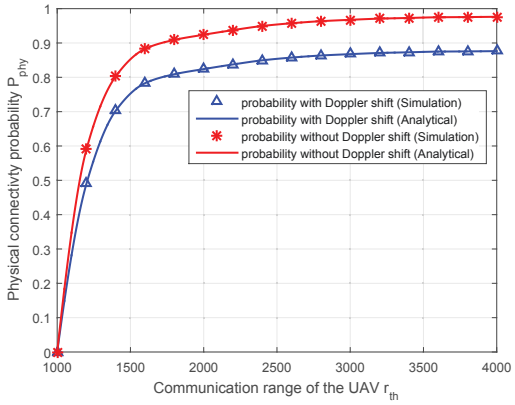


Figure 5.10 : Physical connectivity probability P_{phy} vs. Communication range r_{th}

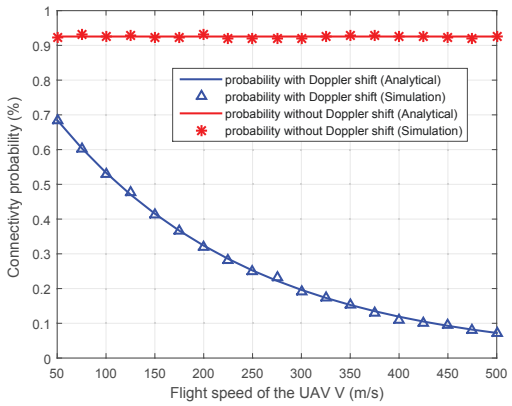


Figure 5.11 : Physical connectivity probability P_{phy} vs. Speed V

how the probability changes with different parameters: the communication range r_{th} and flight speed V. In order to make the simulation more realistic, we set the carrier frequency at 5 GHz based on IEEE 802.11n, and assume that Doppler shift threshold of the receiver is 1000 Hz.

As illustrated in Fig. 10, we can see that with r_{th} increasing from 1000 m to 4000 m, the physical connectivity probability between neighbor UAVs increases a lot. We also find that the physical connectivity probability with a Doppler shift is significantly lower than without a Doppler shift, which means that the Doppler effect caused by the high-speed movement of UAVs may degrade the network performance. Therefore, it is necessary for us to eliminate the Doppler frequency offset at the receiving end and improve the performance of the UAV Networks.

From Fig. 11, we can see that the flight speed of the UAV has a negative impact on the connectivity between neighbor UAVs, especially when the Doppler shift is taken into consideration. As the speed of the UAV increases, the Doppler frequency offset grows gradually, leading to a continuous decrease in physical connectivity probability.

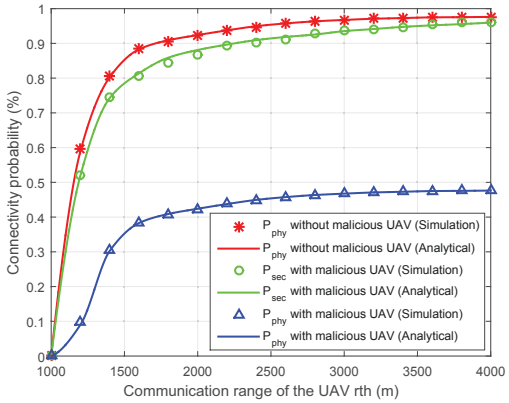


Figure 5.12 : Connectivity probability vs. Communication range r_{th}

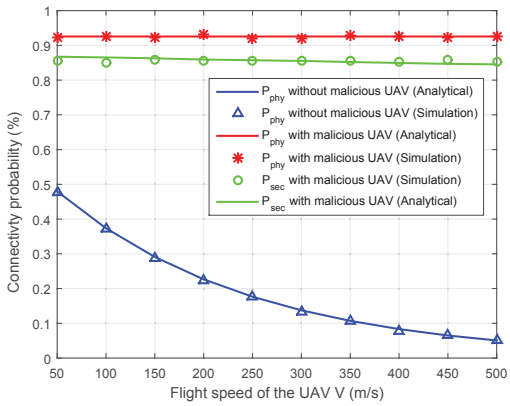


Figure 5.13 : Connectivity probability vs. Communication range r_{th}

5.5.3 Secure Connectivity Probability

In this section, the secure connectivity probability between two UAVs in the UAV Networks is simulated. We compare the secure connectivity probability with the physical connectivity probability in the presence of malicious UAVs. It is assumed that the proportion of malicious UAVs in the network is 30 %.

As shown in Fig. 5.12, with an increase in the communication range r_{th}, both physical and secure connectivity probabilities increase. In addition, the secure connectivity probability P_{sec} between two neighbour UAVs with malicious UAVs is much higher than P_{phy} with malicious UAVs, and is closer to the P_{phy} without malicious

UAVs. The trust evaluation occurring between the subject and object UAV may consume time, energy and other resources, resulting in a slightly lower secure connectivity probability with malicious nodes than without malicious nodes. However, when there are malicious UAVs in the networks, the connectivity probability can be significantly improved with the trust model of UAVs, which can prove the effectiveness of the trust model.

Fig. 5.13 depicts the relationship between connectivity probability in UAV Networks and the flight speed of the UAVs. We can observe that both P_{sec} and P_{phy} remain basically unchanged as the speed increases. In the presence of malicious UAVs, P_{sec} is clearly higher than P_{phy}. Therefore, we can conclude that the proposed trust model has good robustness and reliability, and can effectively improve network performance. According to the theoretical analysis and simulation, we find that the trust model established in this chapter can effectively guarantee secure and reliable communication between UAVs and boost the connectivity probability when the UAV Networks suffer network attacks and other security risks.

5.6 Conclusion

In this chapter, we have proposed a novel trust model that can evaluate the reliability and security of UAV Networks. The trust model is established based on UAV communication behaviors, the characteristics of channels between UAVs and the mobility of UAVs. In addition, it consists of four sections: the direct trust section, indirect trust section, integrated trust section, and trust update section. The secure link in UAV Networks is also presented based on the proposed trust model, and it exists only when both the physical link and the trust link between two UAVs exist. In addition, both physical connectivity probability and secure connectivity probability between two UAVs in the presence of the Doppler shift have been derived. Simulation results show that compared to the physical connection probability with

or without malicious attacks, the proposed trust model can effectively ensure secure communication and reliable connectivity between UAVs and enhance network performance when the UAV Networks suffer malicious attacks and other security risks. In our future work, we will apply our trust model to routing protocol design in UAV Networks.

Chapter 6

Secrecy Performance Analysis of Terrestrial Radio Links against Aerial Eavesdroppers

6.1 Introduction

In this chapter, we study the threat that an aerial eavesdropper can pose to terrestrial wireless communications, from an information-theoretic point of view. It would be of particular interest to understand the robustness of terrestrial wireless communications under exposure to new threats from aerial adversaries, such as aerial eavesdroppers [16]. The attractive advantages or merits of UAVs, such as excellent flexibility, maneuverability and mobility, as well as elevated positions, can potentially increase security risks that UAVs could adversely pose [17]. Despite a significant amount of research efforts on physical layer security in wireless communications, aerial adversaries have drawn little attention. The secrecy performance, captured by ergodic secrecy capacity, secrecy outage probability, or outage secrecy capacity [98, 99, 44], has yet to be understood in the presence of aerial eavesdroppers with unprecedented mobility and maneuverability in 3D spaces [16].

This chapter studies the threat an aerial eavesdropper can pose to terrestrial wireless communications from an information-theoretic perspective. The (spatio-temporally) achievable ergodic secrecy rate (or "ergodic secrecy rate" for brevity) and the average ϵ-outage secrecy rate are analyzed for a transmitter-receiver pair on the ground, in the case where an aerial eavesdropper flies a random trajectory with STs in 3D spherical spaces. Closed-form asymptotic approximations of the secrecy rates are derived based on the almost sure convergence and non-trivial mathematical

manipulations.

Validated by extensive simulations, our analysis provides tight results for the ergodic secrecy rate and ϵ-outage secrecy rate of the ground transmitter-receiver pair spied on by an aerial eavesdropper. An important finding of this chapter indicates that ground transmissions are inherently vulnerable to aerial eavesdropping which can be carried out in a distance without being noticed. Critical 3D spherical regions are identified, within which the aerial eavesdropper is able to overhear all the ground transmissions, and the ergodic and the average ϵ-outage secrecy rates vanish.

The rest of this chapter is organized as follows. In Sec. 6.2, the system model is described. In Sec. 6.3, we first analyze the ergodic and the average ϵ-outage secrecy rates of a ground transmitter-receiver pair in the presence of an aerial eavesdropper following the ST mobility model, and then extend the analysis to the practical case where path loss model is non-isotropic and the ground transmitter antenna is not omni-directional. In Sec. 6.4, simulation results are presented to validate the accuracy of our analysis, followed by concluding remarks in Sec. 6.5.

6.2 System Model

6.2.1 Mobility Model

We assume that an aerial eavesdropper, e.g., a UAV, flies a random 3D trajectory following the ST Mobility Model [59, 60]. The model decouples the movement of the UAV between the horizontal directions, i.e., along the x- and y-axes, and the vertical direction, i.e., along the z-axis [59]. On the horizontal plane, the UAV randomly chooses a turn center to circle around at a constant speed until the next turn center is selected. The duration of the UAV circling around a turn center is exponentially distributed. The next turn center is picked up on the line perpendicular to the instantaneous heading direction of the UAV. This ensures the smoothness of the

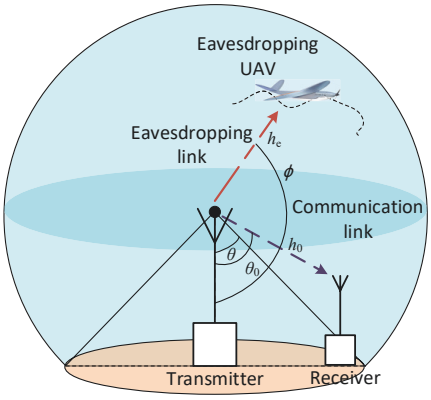


Figure 6.1 : The system of interest, where there is a pair of legitimate transmitter and receiver on the ground, and an aerial eavesdropper flying within the transmission range of the transmitter. The eavesdropper follows the ST mobility model.

flight trajectories. Furthermore, the ST mobility model assumes that the inverse of the radius of every turn follows a zero-mean Gaussian distribution with a small variance. In the vertical direction, i.e., along the z-axis, the UAV is assumed to maintain a constant acceleration while circling around a turning center. The relevant parameters in this model can be estimated from experimental flight test data and measurements. It has been proved in [59, 60] that the ST mobility model has a uniform stationary distribution of the position of the UAV within a 3D finite space.

The scenario of interest is that the aerial eavesdropper flies with the random ST trajectory within a 3D spherical cap centered at a ground transmitter, as illustrated in Fig. 6.1. The 3D spherical cap specifies the coverage region of the ground transmitter. For illustration convenience, the transmitter, the receiver and the aerial eavesdropper are assumed to be equipped with a single omni-directional antenna; unless otherwise specified.

The PDF of the transmitter-eavesdropper distance l_e, denoted by $f_{l_e}(\tau)$, is given by (see Appendix 6.6.1)

$$f_{l_e}(\tau) = \frac{2(1+\cos\theta)\cos^2\theta + \sin^2\theta}{2(1+\cos\theta)\cos^2\theta + \sin^2\theta\cos^3\theta}\frac{3\tau^2}{r^3}, \text{ for } 0 \le \tau \le r\cos\theta; \tag{6.1}$$

$$f_{l_e}(\tau) \approx \frac{2(1+\cos\theta)(1-\cos^3\theta)+\sin^2\theta\cos\theta}{2(1+\cos\theta)(1-\cos^3\theta)+\sin^2\theta\cos\theta(1-\cos^3\theta)}\frac{3\tau^2}{r^3}, \text{ for } r\cos\theta \le \tau \le r. \tag{6.2}$$

Accordingly, the expectation of the transmitter-eavesdropper distance, denoted by $\bar{l}_e$, is given by (see Appendix 6.6.1)

$$\begin{aligned} \bar{l}_e &\approx \frac{3}{4}\left[1+\frac{\sin^2\theta\cos\theta}{\sin^2\theta\cos\theta+2(1+\cos\theta)}\right] r, \text{ if } 0<\theta<\frac{\pi}{2}; \\ \bar{l}_e &= \frac{3}{4}r, \text{ if } \theta = 0 \text{ or } \theta = \frac{\pi}{2}, \end{aligned} \tag{6.3}$$

where r is the radius of the spherical cap accounting for the transmission range of the ground transmitter; and $\theta \in [0, \frac{\pi}{2}]$ is the polar angle of the spherical cap.

Apart from the ST mobility model, other existing mobility models include the Random Directional (RD) [100], Three-Way Random [101], Semi-Random Circular Movement (SRCM) [102], and Flight Plan (FP) models [103]. All the models can support a good level of mobility and maneuverability. They are random processes, except for the FP model which is deterministic. With the consideration on aerodynamics, the SRCM, Three-Way Random, and FP models were also designed for UAVs with constraints on the turn center and radius, and trajectory of the UAV, respectively [60, 59, 102, 101, 103]. The SRCM has a predefined turn center and various radii [102]. The Three-Way Random model has constant heading speed and turn radius [101]. The FP model has predefined trajectory plans [103]. In contrast, the RD model is a generic mobility model. Although extended for UAVs, the RD model undergoes sharp turns and may not comply with aerodynamic and mechanical constraints [100].

None of the existing UAV mobility models were designed for UAV eavesdroppers though. The UAV eavesdroppers are expected to disguise their intention of eavesdropping by flying random trajectories in 3D spaces. An entropy-based measure was developed in [60] to quantify the trajectory randomnesses of different mobility

models. It was reported in [60] that the ST mobility model is only next to the RD model which does not account for the maneuverability of UAVs. It was also reported in [60] that the FP, SRCM, and Three-Way mobility models yield lower randomnesses than the ST mobility model and they are more structured and noticeable. This is because the SRCM and the Three-Way mobility models have predefined turn centers and radii [59], while the FP model has deterministic flight patterns [103], as mentioned earlier.

The ST mobility model can serve as the worst-case mobility model for practical aerial eavesdroppers, in the sense that further optimizations of the mobility patterns can improve the eavesdropping performance. Such optimizations would require both the eavesdropping rate and the furtiveness of the eavesdroppers to be taken into account, and have yet to be studied in the literature.

6.2.2 Channel Model

The channels from the ground transmitter, to the receiver and aerial eavesdropper, consist of small-scale channel fading and path loss. The small-scale channel coefficient between the ground transmitter and receiver, denoted by h_0, is assumed to follow the Rician fading with the Rician factor $K \geq 0$ (where $K = 0$ for the Rayleigh fading). The small-scale channel coefficient between the ground transmitter and the aerial eavesdropper, denoted by h_e, is assumed to follow the Rician fading with the Rician factor $K_e > 0$, since LoS prevails in open spaces. L and α are the distance and the path loss exponent of the ground-to-ground (G2G) link, respectively. l_e and α_e are the distance and the path loss exponent of the G2U link, respectively.

As modeled in [61, 104], the path loss from the ground transmitter to the aerial eavesdropper depends on the elevation angle in-between. Let $\phi \in \left[-\frac{\pi}{2}, \frac{\pi}{2}\right]$ denote the elevation angle. For $0 \leq \phi \leq \frac{\pi}{2}$, the path loss exponent, denoted by $\alpha_e(\phi)$, can

be modeled as [61]

$$\alpha_e(\phi) = a_1 \cdot \mathcal{P}_{\text{LoS}}(\phi) + b_1, \tag{6.4}$$

where $\mathcal{P}_{\text{LoS}}(\phi) = \frac{1}{1+a_2 \exp(-b_2\phi)}$; and the model parameters a_1, a_2, b_1 and b_2 depend on the environment and the carrier frequency [61, 104]:

$$\begin{aligned} a_1 &= \frac{\alpha_{\frac{\pi}{2}} - \alpha_0}{\mathcal{P}_{\text{LoS}}(\frac{\pi}{2}) - \mathcal{P}_{\text{LoS}}(0)};\ b_1 = \alpha_0 - a_1 \mathcal{P}_{\text{LoS}}(0); \\ a_2 &= \sum_{j=0}^{3} \sum_{i=0}^{3-j} c_{ij}^a (\beta_1\beta_2)^i \beta_3^j;\ b_2 = \sum_{j=0}^{3} \sum_{i=0}^{3-j} c_{ij}^b (\beta_1\beta_2)^i \beta_3^j, \end{aligned} \tag{6.5}$$

where coefficients c_{ij}^a and $c_{ij}^b, \forall\, i, j$, are given in [104, Tabs. I & II]; β_1, β_2 and β_3 are environment-dependent variables, and four selected urban environment, i.e., Suburban $(0.1, 750, 8)$, Urban $(0.3, 500, 15)$, Dense Urban $(0.5, 300, 20)$, and Highrise Urban $(0.5, 300, 50)$ for β_1, β_2 and β_3, respectively, are provided in [104]. We set $\alpha_0 = \alpha_e(0)$ and $\alpha_{\frac{\pi}{2}} = \alpha_e(\frac{\pi}{2})$. For $-\frac{\pi}{2} \leq \phi < 0$, we assume $\alpha_e(\phi) = \alpha_e(0)$.

The ground transmitter may also be equipped with a directional antenna. Let $\mathcal{G}(\phi)$ denote the antenna gain of the ground transmitter in the direction of the aerial eavesdropper. It is reasonable to assume that $\mathcal{G}(\phi)$ first increases in $\left[-\frac{\pi}{2}, \theta_0\right)$ and then decreases in $\left(\theta_0, \frac{\pi}{2}\right]$. θ_0 is the pointing direction of the antenna of the ground transmitter, as depicted in Fig. 6.1.

The received signals at the ground receiver and the eavesdropper, denoted respectively by y_r and y_e, are given by

$$y_r = \sqrt{PL^{-\alpha}} h_0 x_s + n_r; \tag{6.6}$$

$$y_e = \sqrt{P\mathcal{G}(\phi) l_e^{-\alpha_e(\phi)}} h_e x_s + n_e, \tag{6.7}$$

where x_s has a circularly symmetric complex Gaussian distribution $\mathcal{CN}(0, 1)$, i.e., $\mathbb{E}\left[\, |x_s|^2 \,\right] = 1$, $|\cdot|$ stands for norm, and $\mathbb{E}\left[\cdot\right]$ denotes expectation; P is the transmit

power of the ground transmitter; n_r and n_e are the AWGNs with $\mathbb{E}\left[|n_r|^2\right] = \sigma_r^2$ and $\mathbb{E}\left[|n_e|^2\right] = \sigma_e^2$, respectively.

Therefore, the instantaneous SNR at the ground receiver, denoted by ζ_r, can be written as

$$\zeta_r = PL^{-\alpha}|h_0|^2/\sigma_r^2. \tag{6.8}$$

The instantaneous SNR at the aerial eavesdropper, denoted by ζ_e, is given by

$$\zeta_e = Pl_e^{-\alpha_e(\phi)}\mathcal{G}(\phi)|h_e|^2/\sigma_e^2. \tag{6.9}$$

In a special case, $a_2 = 0$ (in turn, $\alpha_e(\phi) = \alpha_e$) and $\mathcal{G}(\phi) = 1$; in other words, both the path loss and the transmitter antenna gain are isotropic. (6.9) can be rewritten as

$$\zeta_e = Pl_e^{-\alpha_e}|h_e|^2/\sigma_e^2. \tag{6.10}$$

It is assumed that no CSI of the legitimate and eavesdropping channels is available at the transmitter, i.e., no CSI-at-the-Transmitter (CSIT). This is because the aerial eavesdropper flies a random trajectory to disguise its intention of eavesdropping. Leave alone returning any CSI of the eavesdropping channel. The legitimate transmitter may not be aware of the existence of the eavesdropper, and keeps transmitting the full power P. It is also assumed that perfect CSI is available at the ground receiver and the aerial eavesdropper. Both the receiver and eavesdropper can estimate their CSI based on pilot signals, and then detect the information signals by using coherent detection. In the rest of this chapter, the achievable ergodic and outage secrecy rates with no CSIT are analyzed, and shown to asymptotically converge to their counterparts with perfect CSIT in high SNR regimes. The 3D regions are identified within which an aerial eavesdropper with the ST mobility model can have the legitimate ground link completely exposed.

6.3 Average Achievable Secrecy Rate in the Presence of an Aerial Eavesdropper

In this section, closed-form expressions for the (spatio-temporally) achievable ergodic and the average ϵ-outage secrecy rates of the G2G link are derived in the presence of an aerial eavesdropper following the ST mobility model. The research approach we take here is to first analyze the temporally ergodic secrecy rate and the instantaneous outage secrecy rate with respect to a specific distance of the eavesdropper to the ground transmitter l_e. Then, we apply the almost sure ($a.s.$) convergence to replace l_e with its expectation and derive closed-form approximations or bounds for the (spatio-temporally) ergodic secrecy rate and the average outage secrecy rate with the mobility of the aerial eavesdropper captured.

For illustration convenience, we start with a simple case where the path loss between the ground transmitter and the aerial eavesdropper is isotropic and the ground transmitter has an omni-directional antenna (i.e., $\alpha_e(\phi) = \alpha_e$ and $\mathcal{G}(\phi) = 1$). Then, we show that the conclusions drawn in the simple case can be readily extended to the general cases where the path loss depends on the elevation angle (as modeled in [61, 104]), and the ground transmitter antenna is not omni-directional.

6.3.1 Ergodic Secrecy Rate

The achievable secrecy rate can be define as [58]

$$\mathcal{C}^s_{\text{erg}} = \mathbb{E}\left[\mathcal{C}^s\right] = \mathbb{E}\left[\left[\log_2\left(1+\zeta_r\right) - \log_2\left(1+\zeta_e\right)\right]^+\right], \tag{6.11}$$

where $[x]^+ = \max\{x, 0\}$. (6.11) measures the secrecy loss of the legitimate link to a seemingly harmless UAV to which the legitimate transmitter and receiver pay little attention.

In high SNR regimes (i.e., $\zeta_r, \zeta_e \gg 1$), the achievable ergodic secrecy rate with no CSIT can asymptotically approach that with perfect CSIT, with the growth of the SNR. This is because the legitimate transmitter and receiver, and the eavesdropper are assumed to be equipped with a single antenna, and the ergodic secrecy rate with perfect CSIT would be achieved by optimizing the transmit power P based on the perfect CSIT of both the legitimate and eavesdropping channels. When $\zeta_r, \zeta_e \gg 1$, however, $\mathbb{E}\left[\max_P \left[\log_2\left(1+\zeta_r\right) - \log_2\left(1+\zeta_e\right)\right]^+\right] \to \mathbb{E}\left[\left(\log_2\left(\frac{\zeta_r}{\zeta_e}\right)\right)^+\right] = \mathbb{E}\left[\left(\log_2\left(\frac{|h_0|^2 L^{-\alpha}/\sigma^2}{|h_e|^2 l_e^{-\alpha_e}/\sigma_e^2}\right)\right)^+\right]$. The ergodic secrecy rate with perfect CSIT becomes independent of P. The achievable ergodic secrecy rate with no CSIT converges to that with perfect CSIT.

Given the eavesdropper's location, we first evaluate the temporally ergodic secrecy rate with no CSIT. In Rician fading channels and isotropic UAV path loss model, (6.11) can be given as follows.

Lemma 5. *Suppose that the channel coefficients h_0 and h_e follow the Rician distributions with parameters K and K_e, respectively. Given L and l_e, the temporally ergodic secrecy rate of the G2G link with no CSIT can be approximated by*

$$\mathcal{C}_{\text{erg}}^{s} \approx \log_2\left(\frac{P\sigma_e^2 L^{-\alpha} + \sigma_r^2\sigma_e^2}{P\sigma_r^2 l_e^{-\alpha_e} + \sigma_r^2\sigma_e^2}\right) \triangleq \mathcal{C}_{\text{erg}}\left(L, l_e\right). \tag{6.12}$$

If $\sigma_r^2 = \sigma_e^2 = \sigma^2$, then $\mathcal{C}_{\text{erg}}^{s} \approx \log_2\left(\frac{PL^{-\alpha}+\sigma^2}{Pl_e^{-\alpha_e}+\sigma^2}\right)$.

Proof. See Appendix 6.6.2. □

In Lemma 5, the approximation is in fact increasingly accurate with the *a.s.* convergence, i.e., $C_{\text{erg}}^{s} \xrightarrow{a.s.} C_{\text{erg}}(L, l_e)$, as the numbers of antennas increase at the ground receiver and the aerial eavesdropper where maximal ratio combining (MRC) is carried out. The proof of the lemma is based on the *a.s.* convergence, when these antenna numbers are large; see Appendix 6.6.3. The approximation is taken here,

since we set the antenna numbers to be one to focus on the impact of the eavesdropper's mobility on the confidentiality of the legitimate ground link. Lemma 5 can be asymptotically accurate, e.g., in future millimeter wave (mmWave) communications with increasingly large numbers of antennas at the legitimate receiver and the eavesdropper.

Given $\mathcal{C}_{\text{erg}}(L, l_e)$, we can derive the (spatio-temporally) ergodic secrecy rate $\mathbb{E}_{l_e}[\mathcal{C}_{\text{erg}}(L, l_e)]$ with the mobility of the aerial eavesdropper captured, by non-trivial mathematical manipulations.

Theorem 6. *In the presence of an aerial eavesdropper with a random 3D trajectory following the ST mobility model, (i.e., the location of the eavesdropper has a random uniform distribution), the (spatio-temporally) ergodic secrecy rate of the G2G link with no CSIT can be approximated by*

$$\mathbb{E}_{l_e}\left[\mathcal{C}_{\text{erg}}\left(L, l_e\right)\right] \approx \mathcal{C}_{\text{erg}}\left(L, \bar{l}_e\right) = \log_2\left(\frac{P\sigma_e^2 L^{-\alpha} + \sigma_r^2\sigma_e^2}{P\sigma_r^2\left(\bar{l}_e\right)^{-\alpha_e} + \sigma_r^2\sigma_e^2}\right), \tag{6.13}$$

where the approximation error can asymptotically diminish with the increase of the radius of the aerial eavesdropper's flight zone, r, and the antenna numbers of the legitimate receiver and aerial eavesdropper.

Proof. See Appendix 6.6.4. □

Suppose that $\sigma_e^2 = \sigma_r^2 = \sigma^2$. The radius of the aerial eavesdropper's flight region, r_c, within which the ergodic secrecy rate is zero, is $r_c \approx \frac{2}{3}\left[\frac{\sin^2\theta\cos\theta + 2(1+\cos\theta)}{\sin^2\theta\cos\theta + \cos\theta + 1}\right] L^{\frac{\alpha}{\alpha_e}}$. If $r > r_c$, then $\mathcal{C}_{\text{erg}}\left(L, \bar{l}_e\right) > 0$; otherwise, $\mathcal{C}_{\text{erg}}\left(L, \bar{l}_e\right) = 0$. The G2U link between the aerial eavesdropper and the ground transmitter is likely to be an LoS path. In most cases, $\alpha_e \leq \alpha$. Under this circumstance, we have $r_c \geq \frac{2}{3}\left[\frac{\sin^2\theta\cos\theta + 2(1+\cos\theta)}{\sin^2\theta\cos\theta + \cos\theta + 1}\right] L$. As long as flying randomly in the 3D space with the radius $r < \frac{2}{3}\left[\frac{\sin^2\theta\cos\theta + 2(1+\cos\theta)}{\sin^2\theta\cos\theta + \cos\theta + 1}\right] L$, the aerial eavesdropper can overhear all the transmission of the ground transmitter.

In high SNR regimes, i.e., $P \gg \sigma^2$, the achievable ergodic secrecy rate with no CSIT depends on the distances L and $\bar{l}_e$, and path loss exponents α and α_e, and is independent of the transmit power of the ground transmitter P, as can also be shown in (6.13). As mentioned earlier, the achievable ergodic secrecy rate with no CSIT can asymptotically converge to that with perfect CSIT in the high SNR regimes.

6.3.2 Average ϵ-Outage Secrecy Rate

The secrecy outage probability defines the probability that the instantaneous secrecy rate with no CSIT is lower than a secrecy rate threshold $x > 0$, and can be evaluated [45]

$$\begin{aligned} \mathcal{P}_{\text{out}}^{s}(x) &= \Pr\left(\mathcal{C}^{s} < x\right) \\ &= \Pr\left\{\left[\log_2\left(1+\zeta_r\right) - \log_2\left(1+\zeta_c\right)\right]^{+} < x\right\}. \end{aligned} \tag{6.14}$$

The ϵ-outage secrecy rate is the secrecy rate threshold x, denoted by $\mathcal{C}_{\text{out}}^{\text{s}}$, under which the secrecy outage probability $\mathcal{P}_{\text{out}}^{\text{s}}\left(\mathcal{C}_{\text{out}}^{\text{s}}\right) = \epsilon$. By substituting (6.8) and (6.10) into (6.14), the secrecy outage probability can be rewritten as

$$\Pr\left\{\Psi < 2^{\mathcal{C}_{\text{out}}^{s}} - 1\right\} = \epsilon, \tag{6.15}$$

where $\Psi = \zeta_r - 2^{\mathcal{C}_{\text{out}}^{s}}\zeta_e = \frac{PL^{-\alpha}|h_0|^2}{\sigma_r^2} - \frac{2^{\mathcal{C}_{\text{out}}^{s}} Pl_e^{-\alpha_e}|h_e|^2}{\sigma_e^2}$.

The ground transmitter-receiver pair are likely to experience non-line-of-sight (NLoS). The fading is typically assumed to follow the Rayleigh distribution, i.e., $K = 0$ [105]. Given a location of the aerial eavesdropper and the isotropic UAV path loss model, the ϵ-outage secrecy rate of the ground transmitter-receiver pair is given in the following lemma.

Lemma 6. *Given a location of the eavesdropper and an outage probability ϵ, the*

ϵ-outage secrecy rate of the G2G link with no CSIT can be approximated by

$$\mathcal{C}_{\text{out}}^{s} \approx \mathcal{C}_{\text{out}}\left(L, l_e\right) = \begin{cases} \log_2\left[\dfrac{\left(1+K_e\right)\left(K_e - W_0\right)\sigma_e^2 L^{-\alpha}}{W_0 \sigma_r^2 l_e^{-\alpha_e}}\right], & \text{if } K_e > 0; \\ \log_2\left[\dfrac{\sigma_r^2\sigma_e^2 + \epsilon P \sigma_e^2 L^{-\alpha}}{\sigma_r^2\sigma_e^2 + \left(1-\epsilon\right) P \sigma_r^2 l_e^{-\alpha_e}}\right], & \text{if } K_e = 0, \end{cases} \tag{6.16}$$

where $W_0 = \mathcal{W}_0\left(\frac{K_e \exp(K_e)(1-\epsilon)PL^{-\alpha}}{\sigma_r^2 + PL^{-\alpha}}\right)$*, and* $\mathcal{W}_0\left(\cdot\right)$ *is the principal branch of the Lambert W function*[*].

Proof. See Appendix 6.6.5. □

With Lemma 6, we can use the similar techniques used to prove Theorem 6 here to achieve the average ϵ-outage secrecy rate of the G2G link in which the mobility of the aerial eavesdropper is taken into account.

Theorem 7. *In the presence of an aerial eavesdropper following the ST mobility model, the average ϵ-outage secrecy rate of the G2G link with no CSIT can be approximated by*

$$\begin{aligned} \mathbb{E}_{l_e}\left[\mathcal{C}_{\text{out}}\left(L, l_e\right)\right] &\approx \mathcal{C}_{\text{out}}\left(L, \bar{l}_e\right) \\ &= \begin{cases} \log_2\left[\dfrac{\left(1+K_e\right)\left(K_e - W_0\right)\sigma_e^2 L^{-\alpha}}{W_0 \sigma_r^2 \left(\bar{l}_e\right)^{-\alpha_e}}\right], & \text{if } K_e > 0; \\ \log_2\left[\dfrac{\sigma_r^2\sigma_e^2 + \epsilon P \sigma_e^2 L^{-\alpha}}{\sigma_r^2\sigma_e^2 + \left(1-\epsilon\right) P \sigma_r^2 \left(\bar{l}_e\right)^{-\alpha_e}}\right], & \text{if } K_e = 0. \end{cases} \end{aligned} \tag{6.17}$$

The approximation error of (6.17) *can diminish asymptotically with the increase of the radius of the eavesdropper's flight zone r and the antenna numbers of the legitimate receiver and aerial eavesdropper in high SNR regimes.*

Proof. See Appendix 6.6.6. □

[*]There are countable branches of the Lambert W function, denoted by $\mathcal{W}_k\left(\cdot\right)$ for integer k; $\mathcal{W}_0\left(\cdot\right)$ is the principal branch.

Suppose that $\sigma_e^2 = \sigma_r^2 = \sigma^2$. We evaluate the radius of the eavesdropper's flight region, r_c', within which the average ϵ-outage secrecy rate is zero.

$$r_c' \approx \begin{cases} c\left[\dfrac{W_0 L^\alpha}{(1+K_e)(K_e - W_0)}\right]^{\frac{1}{\alpha_e}}, & \text{if } K_e > 0; \\ c\left[\dfrac{(1-\epsilon) L^\alpha}{\epsilon}\right]^{\frac{1}{\alpha_e}}, & \text{if } K_e = 0, \end{cases} \tag{6.18}$$

where $c = \frac{2}{3}\left[\frac{\sin^2\theta\cos\theta + 2(1+\cos\theta)}{\sin^2\theta\cos\theta + \cos\theta + 1}\right]$. If $r > r_c'$, $\mathcal{C}_{\text{out}}\left(L, \bar{l}_e\right) > 0$; otherwise, $\mathcal{C}_{\text{out}}\left(L, \bar{l}_e\right) = 0$.

As discussed in Sec. 6.3.1, in most cases, $\alpha_e \leq \alpha$ and

$$r_c' \geq r_c^* \triangleq \begin{cases} c\left[\dfrac{W_0}{(1+K_e)(K_e - W_0)}\right]^{\frac{1}{\alpha_e}} L, & \text{if } K_e > 0; \\ c\left(\dfrac{1-\epsilon}{\epsilon}\right)^{\frac{1}{\alpha_e}} L, & \text{if } K_e = 0. \end{cases}$$

In other words, if the aerial eavesdropper flies randomly in a 3D spherical cap with the radius $r < r_c^*$, it can overhear $(1-\epsilon)$ ratio of the transmissions of the ground transmitter.

In high SNR regimes, i.e., $P \gg \sigma^2$, the achievable average ϵ-outage secrecy rate is independent of the transmit power of the ground transmitter P, as the ergodic secrecy rate is in Sec. 6.3.1. However, different from the ergodic secrecy rate, the ϵ-outage secrecy rate also depends on the Rician factor of the eavesdropping link K_e and ϵ (in addition to the distances L and $\bar{l}_e$, and the path loss exponents α and α_e on which the ergodic secrecy rate depends).

6.3.3 Ergodic and Outage Secrecy Rates under Practical UAV Channel Model

We note that our analyses are a non-trivial extension of the typical wiretap channel typically involving a stationary eavesdropper. In particular, Lemma 5 gives

the temporally achievable ergodic secrecy rate of the legitimate ground link given a position of the eavesdropper, like the typical wiretap channel. Based on Lemma 5, Theorem 6 derives an asymptotic expression for the (spatio-temporally) achievable ergodic secrecy rate by translating the mobility of the eavesdropper to a random point process. Different from the typical wiretap channel, the theorem devises the upper and lower bounds for the (spatio-temporally) achievable ergodic secrecy rate and proves their asymptotic convergence with the expansion of the eavesdropper's flight zone. Likewise for Lemma 6 and Theorem 7.

Theorems 6 and 7 establish the ergodic and outage secrecy rates of the ground link, under the simplified UAV channel model where the UAV path loss model is isotropic and the ground transmitter antenna is omni-directional. The theorems can be readily extended to the practical model where the path loss depends on the elevation angle of the eavesdropper [61, 104] and the ground transmitter antenna is not omni-directional, as described in Sec. 3.2.1.

Given l_e and ϕ, the temporally ergodic secrecy rate in Lemma 5 is updated as

$$\mathcal{C}_{\text{erg}}^{s} \approx \log_2\left(\frac{P\sigma_e^2 L^{-\alpha}+\sigma_r^2\sigma_e^2}{P\sigma_r^2 l_e^{-\alpha_e(\phi)}\mathcal{G}(\phi)+\sigma_r^2\sigma_e^2}\right) \triangleq \mathcal{C}_{\text{erg}}\left(l_e,\phi\right), \tag{6.19}$$

which can be proved by substituting $\bar{\zeta}_r = \frac{PL^{-\alpha}}{\sigma_r^2}$ and $\bar{\zeta}_e = \frac{Pl_e^{-\alpha_e(\phi)}\mathcal{G}(\phi)}{\sigma_e^2}$ into (6.29) in the proof of Lemma 5, and then proved in the same way as Lemma 5. This is due to the fact that, given ϕ, $\alpha_e(\phi)$ and $\mathcal{G}(\phi)$ are fixed and, with l_e given, $l_e^{-\alpha_e(\phi)}\mathcal{G}(\phi)$ is also fixed (as $l_e^{-\alpha_e}$ is in Lemma 5). We can replace $l_e^{-\alpha_e}$ with $l_e^{-\alpha_e(\phi)}\mathcal{G}(\phi)$ here, and then evaluate the effect of the Rician fading, as done in Lemma 5.

Since l_e is independent of ϕ given ϕ, $\mathbb{E}_{l_e}\left[\mathcal{C}_{\text{erg}}\left(l_e,\phi\right)\right]$ complies with (6.13), and

can be approximated by

$$\begin{aligned}\mathbb{E}_{l_e}\left[\mathcal{C}_{\text{erg}}\left(l_e,\phi\right)\right] &\approx \log_2\left(\frac{P\sigma_e^2 L^{-\alpha}+\sigma_r^2\sigma_e^2}{P\sigma_r^2\left(\bar{l}_e\right)^{-\alpha_e(\phi)}\mathcal{G}(\phi)+\sigma_r^2\sigma_e^2}\right)\\ &= \log_2\left(\frac{P\sigma_e^2 L^{-\alpha}+\sigma_r^2\sigma_e^2}{P\sigma_r^2\left(\bar{l}_e\right)^{-\eta(\phi)}+\sigma_r^2\sigma_e^2}\right),\end{aligned} \tag{6.20}$$

which can be proved in the same way as Theorem 6. $\eta(\phi)=\alpha_e(\phi)-\frac{\ln(\mathcal{G}(\phi))}{\ln(\bar{l}_e)}$ defines the effective path loss exponent with the non-isotropic path loss model and the transmitter antenna gain incorporated. $\eta(\phi)>0$ due to $\mathcal{G}(\phi)\leq 1$ and $\alpha_e(\phi)>0$.

Therefore, the (spatio-temporally) achievable ergodic secrecy rate can be approximated by

$$\begin{aligned}\mathbb{E}_{l_e,\phi}\left[\mathcal{C}_{\text{erg}}(l_e,\phi)\right] &= \mathbb{E}_{\phi}\left\{\mathbb{E}_{l_e}\left[\mathcal{C}_{\text{erg}}\left(l_e,\phi\right)\right]\right\}\\ &\approx \log_2\left(\frac{P\sigma_e^2 L^{-\alpha}+\sigma_r^2\sigma_e^2}{P\sigma_r^2\left(\bar{l}_e\right)^{-\bar{\eta}}+\sigma_r^2\sigma_e^2}\right),\end{aligned} \tag{6.21}$$

where $\bar{\eta}=\mathbb{E}[\eta(\phi)]=\int_{-\frac{\pi}{2}}^{\frac{\pi}{2}}\frac{1}{\pi}\left[\alpha_e(\phi)-\frac{\ln(\mathcal{G}(\phi))}{\ln(\bar{l}_e)}\right]d\phi$. (6.21) can be proved by first proving that $C_{\text{erg}}(l_e,\phi)$ is a decreasing and convex function of $\eta(\phi)$ and an increasing and concave function of $1/\eta(\phi)$, and then following the proof of Theorem 6.

Likewise, the average ϵ-outage secrecy rate of the G2G link is approximated by

$$\mathbb{E}_{l_e,\phi}\left[\mathcal{C}_{\text{out}}(l_e,\phi)\right]\approx\begin{cases}\log_2\left[\dfrac{\left(1+K_e\right)\left(K_e-W_0\right)\sigma_e^2 L^{-\alpha}}{W_0\sigma_r^2\left(\bar{l}_e\right)^{-\bar{\eta}}}\right], & \text{if } K_e>0;\\ \log_2\left[\dfrac{\sigma_r^2\sigma_e^2+\epsilon P\sigma_e^2 L^{-\alpha}}{\sigma_r^2\sigma_e^2+\left(1-\epsilon\right)P\sigma_r^2\left(\bar{l}_e\right)^{-\bar{\eta}}}\right], & \text{if } K_e=0.\end{cases} \tag{6.22}$$

6.4 Simulation and Evaluation

In this section, we conduct extensive simulations to validate our analysis for the secrecy rates of the ground transmission in the presence of an aerial eavesdropper with a 3D trajectory. Without loss of generality, we assume the same receiver noise

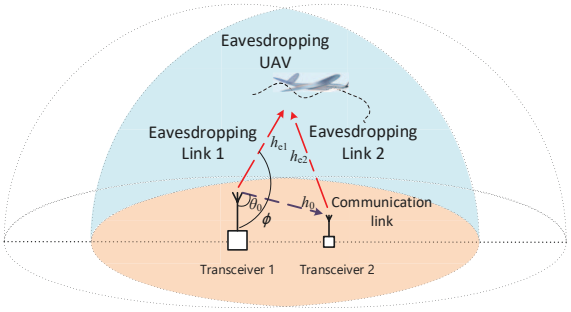


Figure 6.2 : The scenario of a bidirectional ground link, where the aerial eavesdropper flies within the overlapping coverage region of both the legitimate ground nodes.

powers at the ground receiver and the aerial eavesdropper. $\theta = \frac{\pi}{2}$; unless otherwise specified. Other parameters are given in Tab. 6.1 with reference to [72, 70].

Table 6.1 : Simulation parameters

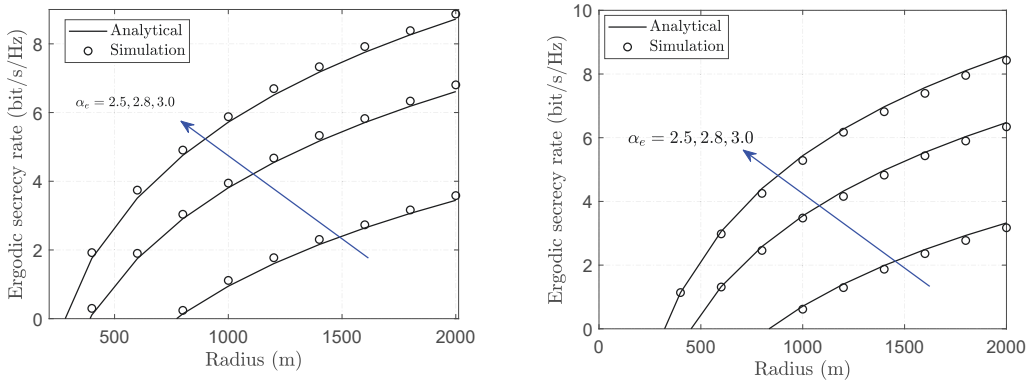
Parameter	Value
Transmit power of the ground transmitter P	20 dBm
Noise power $\sigma_r^2 = \sigma_e^2$	-120 dBm
Path loss exponent α	3.0
Rician factor K_e	0, 10 dB

We note that only the expectation of the transmitter-eavesdropper distance is needed to evaluate the ergodic and ϵ-outage secrecy rates in Theorems 6 and 7; see (6.13) and (6.17). We refer to the scenario captured in the theorems (see Fig. 6.1) as Scenario 1. Theorems 6 and 7 can be readily applied to evaluate another scenario (Scenario 2) where the eavesdropper attempts to eavesdrop on a bidirectional ground link. The eavesdropper flies the ST mobility model within the overlapping coverage region of the two transceivers, as depicted in Fig. 6.2. Assume that the two transceivers are identical and their heights are comparatively negligible to their coverage. The expectation of the transmitter-eavesdropper distance can be numerically

evaluated by (see Appendix 6.6.7)

$$\bar{l}_e^{(2)} = \frac{1}{2}\left[\int_{\frac{L}{2}}^{r} \frac{48\tau^3 - 24L\tau^2}{16r^3 - 12Lr^2 + L^3} d\tau + \int_{\frac{L}{2}}^{r}\int_{0}^{\cos^{-1}\left(\frac{L}{2\tau}\right)} \frac{\sqrt{L^2+\tau^2-2L\tau\cos x}\,(48\tau^2 - 24L\tau)}{\cos^{-1}\left(\frac{L}{2\tau}\right)(16r^3 - 12Lr^2 + L^3)} dx d\tau\right], \tag{6.23}$$

which can be substituted into (6.13) and (6.17) to evaluate the secrecy rate of the bidirectional link.



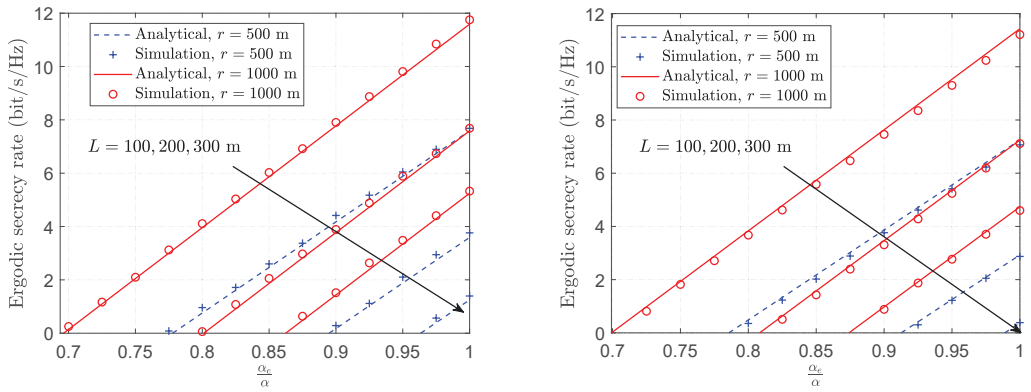
(a) Scenario 1.

(b) Scenario 2.

Figure 6.3 : The ergodic secrecy rate vs. the radius of the eavesdropper's flight region, r, under different values of path loss, α_e, where $L = 200$ m, and $\alpha = 3$.

Fig. 6.3 plots the ergodic secrecy rate in both Scenarios 1 and 2. Along with the analytical results provided in Theorem 1, Monte-Carlo simulation results (i.e., $\mathbb{E}\left[\mathcal{C}^s_{\text{erg}}\right]$) are provided. We simulate the ST mobility model of the eavesdropper for the considered volume and evaluate the expected value of the expression in (6.11), i.e., $\mathbb{E}\left[\mathcal{C}^s_{\text{erg}}\right]$. The number of samples used in the simulations is 5000. We can see that the analytical results coincide with the simulation results, and provide accurate approximations to the ergodic secrecy rate. We also see that the ergodic secrecy rate increases with r. The ergodic secrecy rate also increases with α_e, while the threshold of r, under which the ergodic secrecy rate approaches zero, decreases

with the growth of α_e. In other words, the ground transmission is vulnerable to aerial eavesdropping, especially for the reason that the eavesdropper can implement wiretapping in a distance without being easily noticed or identified.

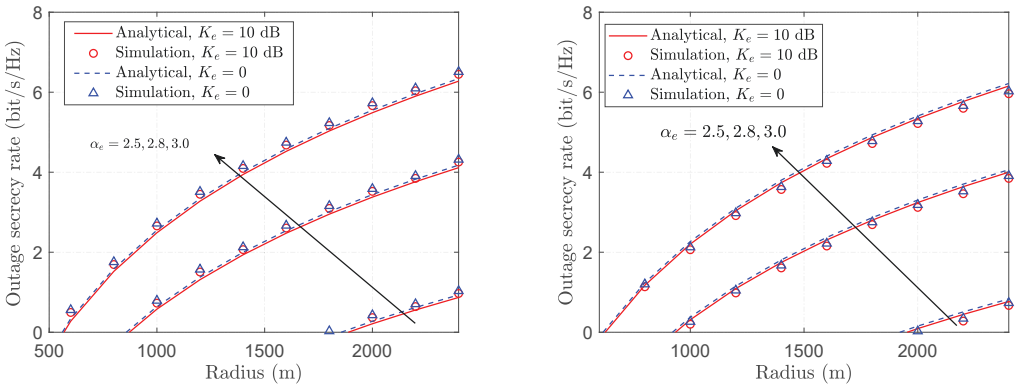


(a) Scenario 1. (b) Scenario 2.

Figure 6.4 : The ergodic secrecy rate vs. $\frac{\alpha_e}{\alpha}$, in the presence of an aerial eavesdropper under different values of path loss exponent, α_e, where $\alpha = 4$.

Fig. 6.4 plots the ergodic secrecy rate of the G2G link, as $\frac{\alpha_e}{\alpha}$ increases. We can see that the secrecy rate increases linearly with $\frac{\alpha_e}{\alpha}$, and the increase rate of the ergodic secrecy rate remains unchanged under different distances between the ground stations, i.e., $L = 100, 200, 300$ m. Moreover, the increase rate rises slowly with the growth of r. With the growth of the distance between the ground stations, the ergodic secrecy rate decreases. We note that the simulation results in Figs. 6.3 and 6.4 are for the exact ergodic secrecy rate, and the approximations developed in Theorem 6 provide fine accuracy, even when the legitimate receiver and the aerial eavesdropper are equipped with a single antenna.

Fig. 6.5 plots the analytical and simulation results for the average ϵ-outage secrecy rate of the G2G link, as the radius of the 3D space the aerial eavesdropper flies, i.e., r, increases. Different values of the Rician factor and path loss exponent are taken for the G2U eavesdropping link. The Rician factor $K_e = 0$ corresponds to



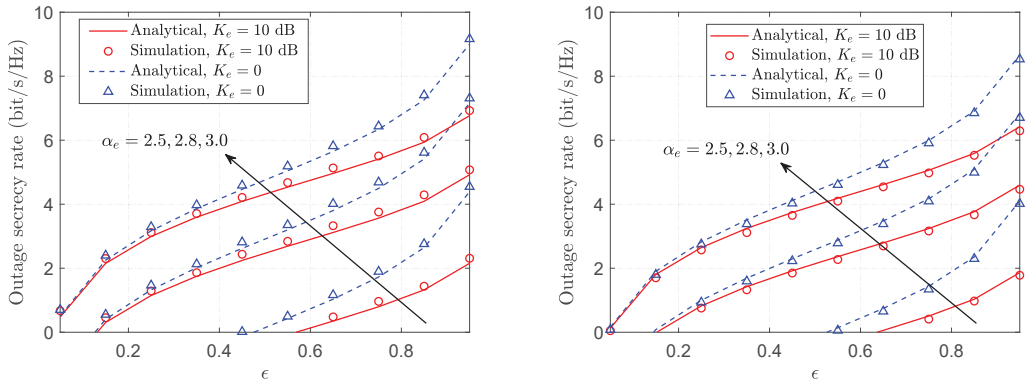
(a) Scenario 1.

(b) Scenario 2.

Figure 6.5 : The ϵ-outage secrecy rate vs. the radius of the eavesdropper's flight region, r, under different values of both path loss exponent and Rician factors, where $\alpha = 3$, $L = 200$ m, and $\epsilon = 0.1$.

the case where there is no LoS path and the channel undergoes the Rayleigh fading. We also set $K_e = 10$ dB in the case where there are an LoS path and NLoS paths between the ground transmitter and the aerial eavesdropper. The NLoS can result from the body blockage of the UAV and the reflection and scattering stemming from buildings or other surrounding infrastructures. The average ϵ-outage secrecy rate is slightly higher in the case of $K_e = 10$ dB than it is in the case of $K_e = 0$. The reason is because the LoS available between the ground transmitter and the aerial eavesdropper facilitates eavesdropping. By comparing the analytical results of Theorem 7, i.e., (6.17), with the simulation results, the accuracy of the analysis is validated.

From Fig. 6.5, we also see that the average ϵ-outage secrecy rate increases with r. The average ϵ-outage secrecy rate decreases as the difference between the G2G path loss exponent, α, and the G2U path loss exponent, α_e, increases. The conclusion drawn is that the eavesdropping from the air can be a particularly severe issue, especially in the case when the eavesdropping link has a strong LoS path with a small path loss exponent.



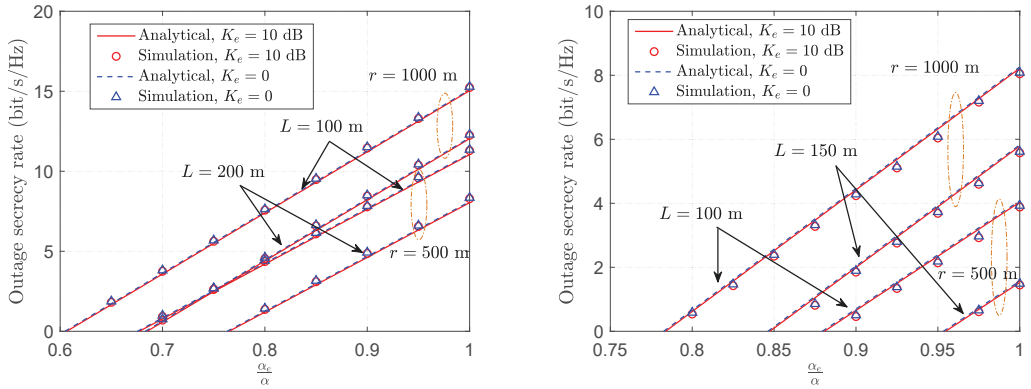
(a) Scenario 1. (b) Scenario 2.

Figure 6.6 : The ϵ-outage secrecy rate vs. the outage probability, ϵ, in the presence of an aerial eavesdropper flying in 3D spherical spaces, where $L = 200$ m, $r = 800$ m, and $\alpha = 3$.

Fig. 6.6 plots the average ϵ-outage secrecy rate against the outage probability, ϵ, under different values of the G2U path loss exponent, α_e. We see that the average ϵ-outage secrecy rate increases with ϵ. Particularly, the larger ϵ is, the higher the secrecy outage rate is required to secure reliable communication. For different values of α_e, the average ϵ-outage secrecy rate has the similar growth rate, and increases quickly with α_e. We also find the average ϵ-outage secrecy rate decreases with the growth of K_e.

Fig. 6.7 depicts the average ϵ-outage secrecy rate against $\frac{\alpha_e}{\alpha}$, under various values of the Rician factor, K_e, and the radius of the 3D space in which the aerial eavesdropper flies, r. We can see that the average ϵ-outage secrecy rate increases linearly with the growth of $\frac{\alpha_e}{\alpha}$, and the increase rate of the secrecy rate remains unchanged at different distances between the ground stations, i.e., $L = 100, 150, 200$ m. The increase rate rises slowly with the growth of r. We also see that the average ϵ-outage secrecy rate decreases slightly with the growth of the Rician factor K_e, since the LoS path becomes increasingly dominant with the growth of K_e.

Fig. 6.8 plots the ergodic and outage secrecy rates of the ground link under non-



(a) Scenario 1.

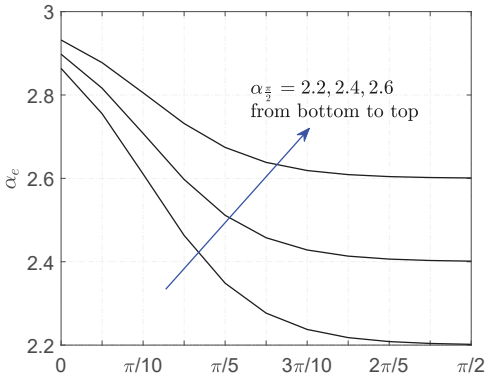
(b) Scenario 2.

Figure 6.7 : The ϵ-outage secrecy rate vs. $\frac{\alpha_e}{\alpha}$, under different values of both target secrecy rate and Rician factor.

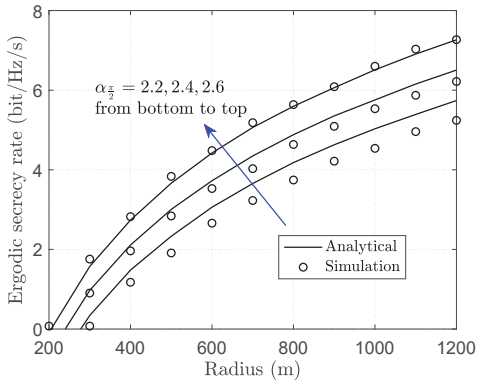
isotropic UAV path loss model described in [104] and a typically assumed squared cosine antenna pattern [106]:

$$\mathcal{G}_{\cos}(\phi) = \begin{cases} \cos^2(\phi - \theta_0), & \text{if } |\phi| \leq \frac{\pi}{2}; \\ 0, & \text{otherwise.} \end{cases}$$

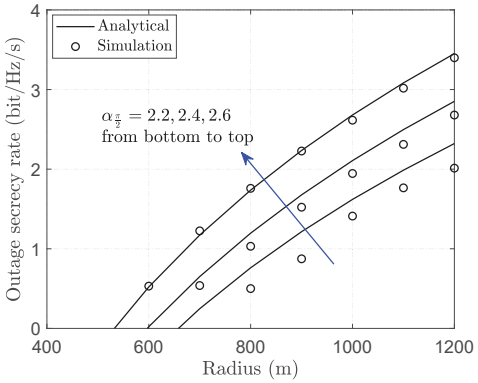
Fig. 6.8(a) shows the change of the path loss exponent α_e against the elevation angle ϕ, where the path loss exponent is $\alpha_0 = 3$ when the eavesdropper and the transmitter are at the same height. We take different values for $\alpha_{\frac{\pi}{2}}$, the path loss exponent when the eavesdropper is right above the transmitter. The smaller $\alpha_{\frac{\pi}{2}}$ is, the clearer the space is and the less influential the ground structures are on the aerial eavesdropper's channel. Figs. 6.8(b) and 6.8(c) plot the ergodic and outage secrecy rates under different values of $\alpha_{\frac{\pi}{2}}$. In general, the secrecy rates grow with the increase of $\alpha_{\frac{\pi}{2}}$ due to the increasing attenuation over the eavesdropping link. Despite being proved to be asymptotically accurate with the growth of r and the antenna numbers at the receiver and eavesdropper, the approximations in Theorems 6 and 7 are shown to provide fine accuracy under isotropic UAV path loss models even with a single



(a) α_e vs. ϕ.



(b) Ergodic secrecy rate.



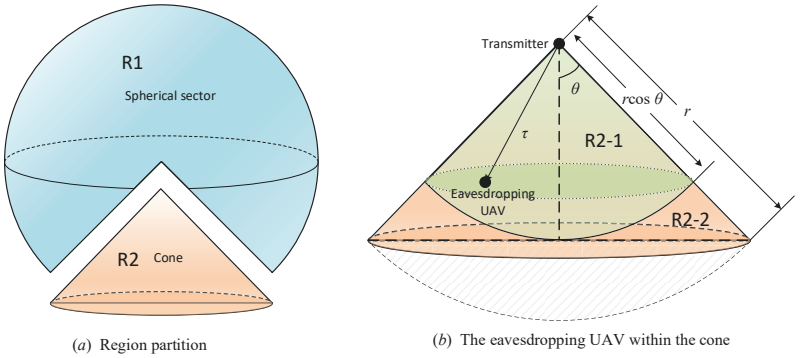
(c) Outage secrecy rate.

Figure 6.8 : The secrecy rates (Scenario 1) under different $\alpha_{\frac{\pi}{2}}$ values, where $L = 200$ m, $K = 0$, $K_e = 10$ dB, and $\alpha_0 = 3$.

antenna at the receiver and eavesdropper in Figs. 6.3 – 6.7. The approximations are less accurate in Figs. 6.8(b) and 6.8(c) under non-isotropic UAV path loss models, due to the additional step dealing with ϕ in (6.21). Better accuracy can be observed when the difference between $\alpha_{\frac{\pi}{2}}$ and α_0 is reduced in Figs. 6.8(b) and 6.8(c).

6.5 Conclusion

In this chapter, we analyzed the ergodic secrecy rate and the average ϵ-outage secrecy rate of a ground transmitter-receiver pair in the presence of an aerial eavesdropper flying along a random trajectory in a 3D spherical region. Closed-form



(a) Region partition (b) The eavesdropping UAV within the cone

Figure 6.9 : Geometric manipulation for the proof of (6.1) – (6.3).

expressions were developed by exploiting the Jensen's inequality and Lambert W function, and validated by simulation results. Our analysis revealed that the ground transmission is vulnerable to aerial eavesdropping which can be carried out in a long distance without being noticed. 3D spherical regions were identified, within which the secrecy rates vanish.

6.6 Appendix

6.6.1 Proof of (6.1) – (6.3)

By dividing the 3D spherical cap into two parts: R1 and R2, as shown in Fig. 6.9(a), we calculate the PDF of l_e, denoted by $f_{l_e}(\tau)$. The volumes of R1 and R2 are $V_1 = \frac{2}{3}\pi(1+\cos\theta)r^3$ and $V_2 = \frac{1}{3}\pi r^3 \sin^2\theta\cos\theta$, respectively. Let $\mathcal{P}_1$ and $\mathcal{P}_2$ denote the probabilities that the eavesdropper is within R1 and R2, respectively. We have

$$\mathcal{P}_1 = \frac{V_1}{V_1+V_2} = \frac{2(1+\cos\theta)}{2(1+\cos\theta)+\sin^2\theta\cos\theta};$$

$$\mathcal{P}_2 = \frac{V_2}{V_1+V_2} = \frac{\sin^2\theta\cos\theta}{2(1+\cos\theta)+\sin^2\theta\cos\theta}.$$

For region R1, we define $\mathcal{P}_{\tau 1}$ as the probability that l_e is shorter than τ. $\mathcal{P}_{\tau 1}$ is equal to the probability that the eavesdropper is located within the spherical sector

with radius τ, and $\mathcal{P}_{\tau 1} = \frac{\tau^3}{d^3}$. *For region R2*, we further divide the region into two parts, i.e., R2-1 and R2-2, as shown in Fig. 6.9(b). The volumes of R2-1 and R2-2 are $V_{21} = \frac{2}{3}\pi r^3(1-\cos\theta)\cos^3\theta$ and $V_{22} = \frac{1}{3}\pi r^3(\cos\theta - 3\cos^3\theta + 2\cos^4\theta)$, respectively. Let $\mathcal{P}_{21}$ and $\mathcal{P}_{22}$ denote the probabilities that the eavesdropper is within R2-1 and R2-2, respectively. We have

$$\mathcal{P}_{21} = \frac{V_{21}}{V_2} = \frac{2(1-\cos\theta)\cos^2\theta}{\sin^2\theta};$$

$$\mathcal{P}_{22} = \frac{V_{22}}{V_2} = \frac{1-3\cos^2\theta+2\cos^3\theta}{\sin^2\theta}.$$

When the aerial eavesdropper is within R2-1, the probability that l_e is shorter than τ is $\mathcal{P}_{\tau 21} = \frac{\tau^3}{r^3\cos^3\theta}$, $0 \le \tau \le r\cos\theta$. When the aerial eavesdropper is within R2-2, the region R2-2 plus the shaded region is used to approximate R2-2 for mathematical tractability, and the probability can be approximated by $\mathcal{P}_{\tau 22} \approx \frac{\tau^3 - r^3\cos^3\theta}{r^3 - r^3\cos^3\theta}$, $r\cos\theta < \tau \le r$.

Now, we can obtain the probability that l_e is shorter than τ within the entire spherical cap. In the case of $0 \le \tau \le r\cos\theta$, the probability $\mathcal{P}_\tau$ and the PDF of l_e are given by

$$\begin{aligned}\mathcal{P}_\tau &= \mathcal{P}_1\mathcal{P}_{\tau 1} + \mathcal{P}_2\mathcal{P}_{21}\mathcal{P}_{\tau 21} \\ &= \frac{2(1+\cos\theta)\cos^2\theta + \sin^2\theta}{2(1+\cos\theta)\cos^2\theta + \sin^2\theta\cos^3\theta}\frac{\tau^3}{r^3};\end{aligned} \tag{6.24}$$

$$f_{l_e}(\tau) = \frac{d\mathcal{P}_\tau}{d\tau} = \frac{2(1+\cos\theta)\cos^2\theta + \sin^2\theta}{2(1+\cos\theta)\cos^2\theta + \sin^2\theta\cos^3\theta}\frac{3\tau^2}{r^3}. \tag{6.25}$$

In the case of $r\cos\theta \le \tau \le r$, $\mathcal{P}_\tau$ and $f_{l_e}(\tau)$ are given by

$$\begin{aligned}\mathcal{P}_\tau &\approx \mathcal{P}_1\mathcal{P}_{\tau 1} + \mathcal{P}_2\mathcal{P}_{22}\mathcal{P}_{\tau 22} \\ &= \frac{2(1+\cos\theta)(1-\cos^3\theta) + \sin^2\theta\cos\theta}{2(1+\cos\theta)(1-\cos^3\theta) + \sin^2\theta\cos\theta(1-\cos^3\theta)}\frac{\tau^3 - r^3\cos^3\theta}{r^3};\end{aligned} \tag{6.26}$$

$$f_{l_e}(\tau) = \frac{d\mathcal{P}_\tau}{d\tau} \approx \frac{2(1+\cos\theta)(1-\cos^3\theta)+\sin^2\theta\cos\theta}{2(1+\cos\theta)(1-\cos^3\theta)+\sin^2\theta\cos\theta(1-\cos^3\theta)}\frac{3\tau^2}{r^3}. \tag{6.27}$$

By using (6.25) and (6.27), the expectation of l_e can be obtained. For $0 < \theta < \frac{\pi}{2}$,

$$\bar{l}_e = \int_0^r \tau f_{l_e}(\tau)d\tau \approx \frac{3}{4}\left[1 + \frac{\sin^2\theta\cos\theta}{\sin^2\theta\cos\theta + 2(1+\cos\theta)}\right] r. \tag{6.28}$$

For $\theta = 0$ or $\theta = \frac{\pi}{2}$, $\bar{l}_e = \frac{3}{4}r$.

6.6.2 Proof of Lemma 5

Since the channel coefficient h_0 and h_e follow the Rician distribution with parameter K and K_e, respectively, the PDFs of ζ_r and ζ_e can be written as [61]

$$f_{\zeta_r}(x) = \frac{1+K}{\bar{\zeta}_r}\exp\left(-K - \frac{(1+K)x}{\bar{\zeta}_r}\right) I_0\left(2\sqrt{\frac{K(1+K)}{\bar{\zeta}_r}x}\right),$$

$$f_{\zeta_e}(y) = \frac{1+K_e}{\bar{\zeta}_e}\exp\left(-K_e - \frac{(1+K_e)y}{\bar{\zeta}_e}\right) I_0\left(2\sqrt{\frac{K_e(1+K_e)}{\bar{\zeta}_e}y}\right),$$

where $I_0(x) = \sum_{n=0}^{\infty} \frac{(x/2)^{2n}}{n!\Gamma(n+1)}$ is the zero-th order modified Bessel function of the first kind [69] and $\Gamma(z) = \int_0^\infty \frac{t^{z-1}}{e^t}dt$ is the Gamma function. $\bar{\zeta}_r$ is the expectation of ζ_r:

$$\begin{aligned}
\bar{\zeta}_r &= \int_0^\infty x f_{\zeta_r}(x)dx \\
&= \frac{1+K}{\bar{\zeta}_r}\exp(-K)\sum_{n=0}^{\infty}\frac{\left(\frac{K(1+K)}{\bar{\zeta}_r}\right)^n}{(n!)^2}\int_0^\infty x^{n+1}\exp\left(-\frac{(1+K)x}{\bar{\zeta}_r}\right)dx \\
&= \frac{\bar{\zeta}_r}{1+K}\exp(-K)\sum_{n=0}^{\infty}\frac{K^n}{(n!)^2}\cdot(n+1)! \\
&= \frac{\bar{\zeta}_r}{1+K}\exp(-K)\cdot(1+K)\exp(K) = \frac{PL^{-\alpha}}{\sigma_r^2}.
\end{aligned}$$

Likewise, $\bar{\zeta}_e$ is the expectation of ζ_e and $\bar{\zeta}_e = \frac{P l_e^{-\alpha_e}}{\sigma_e^2}$ in the special case of $a_2 = 0$. As proved in Appendix 6.6.3, $\mathbb{E}\left[\log_2\left(\frac{\mathcal{X}}{\mathcal{Y}}\right)\right] \xrightarrow{a.s.} \log_2\left(\frac{\mathbb{E}[\mathcal{X}]}{\mathbb{E}[\mathcal{Y}]}\right)$. Therefore, we can obtain

$$\begin{aligned}\mathbb{E}\left[\log_2\left(\frac{1+\zeta_r}{1+\zeta_e}\right)\right] &\xrightarrow{a.s.} \log_2\left(\frac{\mathbb{E}\left[1+\zeta_r\right]}{\mathbb{E}\left[1+\zeta_e\right]}\right) \\ &= \log_2\left(\frac{1+\bar{\zeta}_r}{1+\bar{\zeta}_e}\right) = \log_2\left(\frac{P\sigma_e^2 L^{-\alpha} + \sigma_r^2\sigma_e^2}{P\sigma_r^2 l_e^{-\alpha_e} + \sigma_r^2\sigma_e^2}\right).\end{aligned} \tag{6.29}$$

This concludes the proof of Lemma 5.

6.6.3 Proof of $\mathbb{E}\left[\log_2\left(\frac{\mathcal{X}}{\mathcal{Y}}\right)\right] \xrightarrow{a.s.} \log_2\left(\frac{\mathbb{E}[\mathcal{X}]}{\mathbb{E}[\mathcal{Y}]}\right)$.

To prove this, we consider a generic scenario where the ground receiver and the aerial eavesdropper are equipped with N and N' antennas, respectively. Let x_i $(i = 1, \cdots, N)$ and y_j $(j = 1, \cdots, N')$ be the received SNRs at the different antennas of the ground receiver and the aerial eavesdropper, respectively. They are two sequences of positive square-integrable random variables and not necessarily independent across i or j, $\frac{N'}{N} \to \varepsilon < \infty$. $\mathcal{X} = \sum_{i=1}^{N} x_i$ and $\mathcal{Y} = \sum_{j=1}^{N'} y_j$ are the SNRs of MRC at the ground receiver and the aerial eavesdropper, respectively.

Since $\mathbb{E}[x_i] < \infty$, $i = 1, \cdots, N$, based on *Kolmogorov's* strong law of large numbers, we have [107]

$$\frac{1}{N}\sum_{i=1}^{N} x_i - \frac{1}{N}\sum_{i=1}^{N}\mathbb{E}[x_i] \xrightarrow{a.s.} 0, \text{as } N \to \infty. \tag{6.30}$$

Since $\frac{1}{N}\sum_{i=1}^{N}\mathbb{E}[x_i] = \mathbb{E}\left[\frac{1}{N}\sum_{i=1}^{N} x_i\right] = \frac{1}{N}\mathbb{E}[\mathcal{X}]$, we have $\frac{1}{N}\mathcal{X} - \frac{1}{N}\mathbb{E}[\mathcal{X}] \xrightarrow{a.s.} 0$, as $N \to \infty$ and $\frac{N'}{N} \to \varepsilon$, i.e., $\frac{1}{N}\mathcal{X} \xrightarrow{a.s.} \frac{1}{N}\mathbb{E}[\mathcal{X}]$, as $N \to \infty$. Similarly, we also have $\frac{1}{N'}\mathcal{Y} - \frac{1}{N'}\mathbb{E}[\mathcal{Y}] \xrightarrow{a.s.} 0$, as $N' \to \infty$, i.e., $\frac{1}{N'}\mathcal{Y} \xrightarrow{a.s.} \frac{1}{N'}\mathbb{E}[\mathcal{Y}]$, as $N' \to \infty$.

By using the *Continuous mapping theorem* [108] for a few times, we have

$$\mathbb{E}\left[\log_2\left(\frac{\mathcal{X}}{\mathcal{Y}}\right)\right] \xrightarrow{a.s.} \log_2\left(\frac{\mathbb{E}[\mathcal{X}]}{\mathbb{E}[\mathcal{Y}]}\right), \quad \text{as } N \to \infty \text{ and } \frac{N'}{N} \to \varepsilon. \tag{6.31}$$

From this analysis, we can see that the *a.s.* convergence can be achieved in (6.31), in the case where N and N' are large, for example, the ground receiver and aerial eavesdropper equipped with large number of antennas in a mmWave systems [109, 110]. In the case where a single antenna is considered at the ground receiver and the aerial eavesdropper (as discussed in this chapter), $\mathbb{E}\left[\log_2\left(\frac{\mathcal{X}}{\mathcal{Y}}\right)\right] \approx \log_2\left(\frac{\mathbb{E}[\mathcal{X}]}{\mathbb{E}[\mathcal{Y}]}\right)$, e.g., in Lemma 5.

6.6.4 Proof of Theorem 6

Based on Lemma 5, $\mathcal{C}_{\text{erg}}(L, l_e)$ can be rewritten as

$$\mathcal{H}_1(\mu) = \log_2\left(\frac{P\sigma_e^2 L^{-\alpha} + \sigma_r^2\sigma_e^2}{P\sigma_r^2\mu + \sigma_r^2\sigma_e^2}\right);$$

$$\mathcal{H}_2(\nu) = \log_2\left[\frac{\left(P\sigma_e^2 L^{-\alpha} + \sigma_r^2\sigma_e^2\right)\nu}{P\sigma_r^2 + \sigma_r^2\sigma_e^2\nu}\right],$$

which are achieved by defining $\mu = l_e^{-\alpha_e}$ and $\nu = l_e^{\alpha_e}$. We can obtain

$$\frac{\partial\mathcal{H}_1(\mu)}{\partial\mu} = -\frac{1}{\ln 2}\cdot\frac{P\sigma_r^2}{\left(P\sigma_r^2\mu + \sigma_e^2\sigma_r^2\right)} \leq 0;$$

$$\frac{\partial^2\mathcal{H}_1(\mu)}{\partial\mu^2} = \frac{1}{\ln 2}\cdot\frac{P^2\sigma_r^4}{\left(P\sigma_r^2\mu + \sigma_e^2\sigma_r^2\right)^2} \geq 0.$$

Thus, $\mathcal{H}_1(\mu)$ is a monotonically decreasing and convex function of μ. We also find that

$$\frac{\partial\mathcal{H}_2(\nu)}{\partial\nu} = \frac{1}{\ln 2}\cdot\frac{P\sigma_r^2}{\left(P\sigma_r^2\nu + \sigma_e^2\sigma_r^2\nu^2\right)} \geq 0;$$

$$\frac{\partial^2\mathcal{H}_2(\nu)}{\partial\nu^2} = -\frac{1}{\ln 2}\cdot\frac{P^2\sigma_r^4 + 2P\sigma_r^4\sigma_e^2\nu}{\left(P\sigma_r^2\nu + \sigma_e^2\sigma_r^2\nu^2\right)^2} \leq 0.$$

Thus, $\mathcal{H}_2(\nu)$ is a monotonically increasing and concave function of μ.

Based on the Jensen's inequality (i.e., $\mathbb{E}[f(x)] \geq f(\mathbb{E}[x])$ if $f(x)$ is convex, otherwise $\mathbb{E}[f(x)] \leq f(\mathbb{E}[x])$), the convexity of $\mathcal{H}_1(\mu)$ with respect to μ, and the

concavity of $\mathcal{H}_2(\nu)$ with respect to ν, we have

$$\mathbb{E}\left[\mathcal{H}_1(\mu)\right] \geq \mathcal{H}_1\left(\mathbb{E}\left[\mu\right]\right);\ \mathbb{E}\left[\mathcal{H}_2(\nu)\right] \leq \mathcal{H}_2\left(\mathbb{E}\left[\nu\right]\right). \tag{6.32}$$

Since $\mathcal{H}_1(\mu) = \mathcal{H}_2(\nu)$, we have

$$\begin{aligned} \mathcal{H}_1\left(\mathbb{E}\left[\mu\right]\right) &\leq \mathbb{E}\left[\mathcal{H}_1(\mu)\right] = \mathbb{E}_{l_e}\left[\mathcal{C}_{\text{erg}}(L, l_e)\right] \\ &= \mathbb{E}\left[\mathcal{H}_2(\nu)\right] \leq \mathcal{H}_2\left(\mathbb{E}\left[\nu\right]\right). \end{aligned} \tag{6.33}$$

Since $\mu = l_e^{-\alpha_e}$ and $\nu = l_e^{\alpha_e}$ are both convex with regard to l_e, by using Jensen's inequality, we have

$$\mathbb{E}\left[\mu\right] \geq \left(\bar{l}_e\right)^{-\alpha_e};\ \mathbb{E}\left[\nu\right] \geq \left(\bar{l}_e\right)^{\alpha_e}. \tag{6.34}$$

As $\mathcal{H}_1(\mu)$ and $\mathcal{H}_2(\nu)$ are monotonically decreasing and increasing functions of μ and ν, respectively, we have

$$\begin{aligned} \mathcal{H}_1\left(\mathbb{E}\left[\mu\right]\right) &\leq \mathcal{H}_1\left(\left(\bar{l}_e\right)^{-\alpha_e}\right) = \mathcal{C}_{\text{erg}}\left(L, \bar{l}_e\right) \\ &= \mathcal{H}_2\left(\left(\bar{l}_e\right)^{\alpha_e}\right) \leq \mathcal{H}_2\left(\mathbb{E}\left[\nu\right]\right). \end{aligned} \tag{6.35}$$

Comparing (6.33) and (6.35), we find that $\mathcal{C}_{\text{erg}}\left(L, \bar{l}_e\right)$ lies between the upper and lower bounds of $\mathbb{E}_{l_e}\left[\mathcal{C}_{\text{erg}}(L, l_e)\right]$. We can approximate

$$\mathbb{E}_{l_e}\left[\mathcal{C}_{\text{erg}}(L, l_e)\right] \approx \mathcal{C}_{\text{erg}}\left(L, \bar{l}_e\right) = \log_2\left(\frac{P\sigma_e^2 L^{-\alpha} + \sigma_r^2\sigma_e^2}{P\sigma_r^2\left(\bar{l}_e\right)^{-\alpha_e} + \sigma_r^2\sigma_e^2}\right). \tag{6.36}$$

By substituting the expectation of the transmitter-eavesdropper distance, $\bar{l}_e$, (6.36) can be rewritten as (6.13).

We proceed to evaluate the approximation accuracy of (6.36). By recalling (6.1)

and (6.2) and referring to (6.28), the expectation of $l_e^{\alpha_e}$ and $l_e^{-\alpha_e}$ can be given by

$$\mathbb{E}[l_e^{\alpha_e}] = h_1(r) = \int_0^r \tau^{\alpha_e} f_{l_e}(\tau) d\tau \approx \frac{3\mathcal{D}_1(\theta)}{3+\alpha_e} r^{\alpha_e}; \tag{6.37}$$

$$\mathbb{E}[l_e^{-\alpha_e}] = h_2(r) = \int_0^r \tau^{-\alpha_e} f_{l_e}(\tau) d\tau \approx \frac{3\mathcal{D}_2(\theta)}{3-\alpha_e} r^{-\alpha_e},\ \alpha_e \neq 3, \tag{6.38}$$

where $\mathcal{D}_1(\theta) = (1-(\cos\theta)^{1+\alpha_e}) \frac{2(1+\cos\theta)(1-\cos^3\theta)+\sin^2\theta\cos\theta}{[2(1+\cos\theta)+\sin^2\theta\cos\theta](1-\cos^3\theta)} + (\cos\theta)^{1+\alpha_e} \frac{2(1+\cos\theta)\cos^2\theta+\sin^2\theta}{2(1+\cos\theta)+\sin^2\theta\cos\theta}$ and $\mathcal{D}_2(\theta) = (\cos\theta)^{1-\alpha_e} \frac{2(1+\cos\theta)\cos^2\theta+\sin^2\theta}{2(1+\cos\theta)+\sin^2\theta\cos\theta} + \frac{2(1+\cos\theta)(1-\cos^3\theta)+\sin^2\theta\cos\theta}{[2(1+\cos\theta)+\sin^2\theta\cos\theta](1-\cos^3\theta)} (1-(\cos\theta)^{3-\alpha_e})$. Then, we have

$$\begin{aligned} \mathcal{H}_1(\mathbb{E}[\mu]) &= \log_2\left(\frac{P\sigma_e^2 L^{-\alpha} + \sigma_r^2\sigma_e^2}{P\sigma_r^2 h_2(r) + \sigma_r^2\sigma_e^2}\right) \\ &\approx \log_2\left(\frac{P\sigma_e^2 L^{-\alpha} + \sigma_r^2\sigma_e^2}{\frac{3\mathcal{D}_2(\theta)}{3-\alpha_e} P\sigma_r^2 r^{-\alpha_e} + \sigma_r^2\sigma_e^2}\right); \end{aligned} \tag{6.39}$$

$$\begin{aligned} \mathcal{H}_2(\mathbb{E}[\nu]) &= \log_2\left(\frac{P\sigma_e^2 L^{-\alpha} + \sigma_r^2\sigma_e^2}{P\sigma_r^2 h_1^{-1}(r) + \sigma_r^2\sigma_e^2}\right) \\ &\approx \log_2\left(\frac{P\sigma_e^2 L^{-\alpha} + \sigma_r^2\sigma_e^2}{\frac{3+\alpha_e}{3\mathcal{D}_1(\theta)} P\sigma_r^2 r^{-\alpha_e} + \sigma_r^2\sigma_e^2}\right). \end{aligned} \tag{6.40}$$

Here, $\frac{3+\alpha_e}{3\mathcal{D}_1(\theta)}$ and $\frac{3\mathcal{D}_2(\theta)}{3-\alpha_e}$ are constants given θ and α_e. (6.37) – (6.40) hold strict equality, when $\theta = \frac{\pi}{2}$ (or in other words, the transmitter antenna height is comparatively negligible to the eavesdropper's flight radius r); see (6.3).

The approximation error of (6.36) is no greater than half of the difference between $\mathcal{H}_1(\mathbb{E}[\mu])$ and $\mathcal{H}_2(\mathbb{E}[\nu])$. The error is increasingly negligible with the growth of r, since both $h_1^{-1}(r)$ and $h_2(r)$ are strictly monotonically decreasing functions of r. $\mathcal{H}_1(\mathbb{E}[\mu]) \to \mathcal{H}_2(\mathbb{E}[\nu])$ when $r \gg \left(\frac{3\mathcal{D}_2(\theta)}{3-\alpha_e}\frac{P}{\sigma_e^2}\right)^{1/\alpha_e}$ and $r \gg \left(\frac{3+\alpha_e}{3\mathcal{D}_1(\theta)}\frac{P}{\sigma_e^2}\right)^{1/\alpha_e}$ in (6.39) and (6.40).

6.6.5 Proof of Lemma 6

When h_0 follows the Rayleigh distribution ($K = 0$), i.e., $|h_0|^2 \sim \exp(1)$, and h_e follows the Rician distribution with parameter K_e, the PDF of Ψ is given by

$$f_\Psi(\psi) = \int_0^\infty f_\mathcal{X}(\psi + y) f_\mathcal{Y}(y) dy \tag{6.41a}$$

$$= \frac{B \exp\left(-K_e + \frac{B}{2} - \frac{\psi}{\bar{\mathcal{X}}}\right)}{2K_e \bar{\mathcal{X}}} \int_0^\infty \frac{1}{2} \exp\left(-\frac{y_1 + B}{2}\right) I_0\left(\sqrt{B y_1}\right) dy_1 \tag{6.41b}$$

$$= \frac{B \exp\left(-K_e + \frac{B}{2} - \frac{\psi}{\bar{\mathcal{X}}}\right)}{2K_e \bar{\mathcal{X}}} Q\left(\sqrt{B}, 0\right) \tag{6.41c}$$

$$= \frac{(1+K_e) \exp\left(-\frac{K_e \bar{\mathcal{Y}}}{\bar{\mathcal{Y}} + (1+K_e)\bar{\mathcal{X}}}\right)}{\bar{\mathcal{Y}} + (1+K_e)\bar{\mathcal{X}}} \exp\left(-\frac{\psi}{\bar{\mathcal{X}}}\right), \tag{6.41d}$$

where $\bar{\mathcal{X}} = \bar{\zeta}_r$ and $\bar{\mathcal{Y}} = \bar{\zeta}_e 2^{\mathcal{C}_{\text{out}}^s}$; (6.41b) is obtained by setting $y_1 = Ay = \frac{2\left[(1+K_e)\bar{\mathcal{X}} + \bar{\mathcal{Y}}\right]}{\bar{\mathcal{X}}\bar{\mathcal{Y}}} y$ and $B = \frac{2K_e(1+K_e)\bar{\mathcal{X}}}{\bar{\mathcal{Y}} + (1+K_e)\bar{\mathcal{X}}}$; (6.41c) is based on the definition of the first-order Marcum Q-function [61, Eq. 8], i.e., $Q(\sqrt{a}, \sqrt{b}) = \int_b^\infty \frac{1}{2} \exp(-\frac{x+a}{2}) I_0(\sqrt{ax}) dx$; (6.41d) is due to $Q\left(\sqrt{a}, 0\right) = 1$.

The ϵ-outage secrecy probability can be evaluated based on [78, Eq. 37], as given by

$$\begin{aligned} \epsilon &= \Pr\left(\Psi \leq 2^{\mathcal{C}_{\text{out}}^s} - 1\right) = 1 - \Pr\left(\Psi \geq 2^{\mathcal{C}_{\text{out}}^s} - 1\right) \\ &= 1 - \int_{2^{\mathcal{C}_{\text{out}}^s} - 1}^\infty \frac{(1+K_e) \exp\left(-\frac{K_e \bar{\mathcal{Y}}}{\bar{\mathcal{Y}} + (1+K_e)\bar{\mathcal{X}}}\right)}{\bar{\mathcal{Y}} + (1+K_e)\bar{\mathcal{X}}} \exp\left(-\frac{\psi}{\bar{\mathcal{X}}}\right) d\psi, \end{aligned} \tag{6.42}$$

which, by taking the integration, leads to

$$\epsilon = 1 - \mathcal{M} \exp\left(-\frac{2^{\mathcal{C}_{\text{out}}^s} - 1}{\bar{\mathcal{X}}}\right), \tag{6.43}$$

where, for notational simplicity, $\bar{\mathcal{X}} = \frac{PL^{-\alpha}}{\sigma_r^2}$, $\bar{\mathcal{Y}} = \frac{Pl_e^{-\alpha_e} 2^{\mathcal{C}_{\text{out}}^s}}{\sigma_e^2}$, and $\mathcal{M}$ is defined as

$$\mathcal{M} = \frac{(1+K_e)\,\bar{\mathcal{X}} \exp\left(-\frac{K_e \bar{\mathcal{Y}}}{\bar{\mathcal{Y}} + (1+K_e)\bar{\mathcal{X}}}\right)}{\bar{\mathcal{Y}} + (1+K_e)\bar{\mathcal{X}}}. \tag{6.44}$$

Based on the secrecy outage probability and the definition of ϵ-outage secrecy rate, we have

$$1-\epsilon = \mathcal{M}\exp\left(-\frac{2^{\mathcal{C}^{\mathrm{s}}_{\mathrm{out}}}-1}{\bar{\mathcal{X}}}\right). \tag{6.45}$$

By exploiting $\exp(-x)\approx 1-x$ when x is small, (6.43) can be approximated by

$$(1-\epsilon)\frac{1}{\mathcal{M}} \approx 1-\frac{2^{\mathcal{C}^{\mathrm{s}}_{\mathrm{out}}}-1}{\bar{\mathcal{X}}}. \tag{6.46}$$

Since $\bar{\mathcal{X}}=\bar{\zeta}_r$ and $\bar{\mathcal{Y}}=2^{\mathcal{C}^{\mathrm{s}}_{\mathrm{out}}}\bar{\zeta}_e$, (6.46) can be rewritten as

$$\frac{(1-\epsilon)\left[\bar{\zeta}_e 2^{\mathcal{C}^{\mathrm{s}}_{\mathrm{out}}}+(1+K_e)\,\bar{\zeta}_r\right]}{(1+K_e)\,\bar{\zeta}_r}\exp\left[\frac{K_e\bar{\zeta}_e 2^{\mathcal{C}^{\mathrm{s}}_{\mathrm{out}}}}{\bar{\zeta}_e 2^{\mathcal{C}^{\mathrm{s}}_{\mathrm{out}}}+(1+K_e)\,\bar{\zeta}_r}\right] \approx 1-\frac{2^{\mathcal{C}^{\mathrm{s}}_{\mathrm{out}}}-1}{\bar{\zeta}_r}. \tag{6.47}$$

In the case of $K_e=0$, (6.47) can be rewritten as

$$(1-\epsilon)\left(\bar{\zeta}_r+\bar{\zeta}_e 2^{\mathcal{C}^{\mathrm{s}}_{\mathrm{out}}}\right) \approx \bar{\zeta}_r-\left(2^{\mathcal{C}^{\mathrm{s}}_{\mathrm{out}}}-1\right). \tag{6.48}$$

The ϵ-outage secrecy rate can be approximated by

$$\mathcal{C}^{s}_{\mathrm{out}} \approx \log_2\left[\frac{1+\epsilon\bar{\zeta}_r}{1+(1-\epsilon)\,\bar{\zeta}_e}\right]. \tag{6.49}$$

In the case of $K_e>0$, let $\mathcal{Z}=\frac{\bar{\zeta}_e 2^{\mathcal{C}^{\mathrm{s}}_{\mathrm{out}}}+(1+K_e)\bar{\zeta}_r}{K_e(1+K_e)\bar{\zeta}_r}$, and (6.47) can be rewritten as

$$\mathcal{Z}\exp\left(-\frac{1}{\mathcal{Z}}\right) \approx \frac{\left(1+\bar{\zeta}_r-2^{\mathcal{C}^{\mathrm{s}}_{\mathrm{out}}}\right)\exp\left(-K_e\right)}{K_e\left(1-\epsilon\right)\bar{\zeta}_r} \tag{6.50a}$$

$$\approx \frac{\left(1+\bar{\zeta}_r\right)\exp\left(-K_e\right)}{K_e\left(1-\epsilon\right)\bar{\zeta}_r}, \tag{6.50b}$$

where (6.50b) is due to the fact that $1+\bar{\zeta}_r \gg 2^{\mathcal{C}^{\mathrm{s}}_{\mathrm{out}}}$[†]. By applying the Lambert W

[†]Based on the definition of the ϵ-secrecy outage rate, we have $\log_2\left(1+\bar{\zeta}_r\right)-\log_2\left(1+\bar{\zeta}_e\right) > \mathcal{C}^{\mathrm{s}}_{\mathrm{out}}$, i.e., $1+\bar{\zeta}_r > 2^{\mathcal{C}^{\mathrm{s}}_{\mathrm{out}}}\left(1+\bar{\zeta}_e\right)$. In the high SNR regimes, $P\gg\sigma_r^2$ and $P\gg\sigma_e^2$, thus $1+\bar{\zeta}_e\gg 1$ and $1+\bar{\zeta}_r \gg 2^{\mathcal{C}^{\mathrm{s}}_{\mathrm{out}}}$.

function to (6.50b), we can obtain

$$\mathcal{Z}^{-1} \approx \mathcal{W}_0\left(\frac{K_e \exp\left(K_e\right)\left(1-\epsilon\right)\bar{\zeta}_r}{1+\bar{\zeta}_r}\right) \triangleq W_0. \tag{6.51}$$

Therefore, the ϵ-secrecy outage rate is given by

$$\mathcal{C}_{\text{out}}^{\text{s}} \approx \log_2\left[\frac{\left(1+K_e\right)\left(K_e-W_0\right)\bar{\zeta}_r}{W_0\bar{\zeta}_e}\right] \triangleq \mathcal{C}_{\text{out}}(L, l_e). \tag{6.52}$$

We proceed to prove that the approximations in (6.49) and (6.52) are asymptotically accurate in high SNR regimes, where $P \gg \sigma_r^2$ and $P \gg \sigma_e^2$ (i.e., $\bar{\zeta}_r \gg 1$ and $\bar{\zeta}_e \gg 1$). Specifically,

$$\begin{aligned} W_0 &= \mathcal{W}_0\left(\frac{K_e \exp\left(K_e\right)\left(1-\epsilon\right)PL^{-\alpha}}{\sigma_r^2 + PL^{-\alpha}}\right) \\ &\approx \mathcal{W}_0\left(K_e \exp\left(K_e\right)\left(1-\epsilon\right)\right) \leq \mathcal{W}_0\left(K_e \exp\left(K_e\right)\right) = K_e. \end{aligned}$$

Considering the typical range of the Rician factor $0 < K_e \leq 10$, we have $\frac{(1+K_e)(K_e-W_0)}{W_0} = \left(1+K_e\right)\left(\frac{K_e}{W_0}-1\right) = \Theta\left(1+K_e\right) = \Theta\left(1\right)$[‡]. Since $\bar{\zeta}_e \gg 1$, we have $\frac{(1+K_e)(K_e-W_0)}{W_0\bar{\zeta}_e} = \frac{\Theta(1)}{\bar{\zeta}_e} \ll 1$. Therefore, $\frac{(1+K_e)(K_e-W_0)\bar{\zeta}_r}{W_0\bar{\zeta}_e} \ll \bar{\zeta}_r$ and $1+\bar{\zeta}_r \gg 2^{\mathcal{C}_{\text{out}}^{\text{s}}}$. This validates the approximation accuracy of (6.46) and, in turn, the approximation accuracy of (6.47), (6.49) and (6.50a). By substituting (6.52) into $1+\bar{\zeta}_r - 2^{\mathcal{C}_{\text{out}}^{\text{s}}}$, we have $1+\bar{\zeta}_r - \frac{(1+K_e)(K_e-W_0)\bar{\zeta}_r}{W_0\bar{\zeta}_e} = 1+\bar{\zeta}_r - \frac{\Theta(1)}{\bar{\zeta}_e}\bar{\zeta}_r \approx 1+\bar{\zeta}_r$. The accuracy of the approximation from (6.50a) to (6.50b) is verified, and so is the approximation accuracy of (6.52).

Finally, (6.16) can be obtained by substituting $\bar{\zeta}_r = \frac{PL^{-\alpha}}{\sigma_r^2}$ and $\bar{\zeta}_e = \frac{Pl_e^{-\alpha_e}}{\sigma_e^2}$ into (6.49) and (6.52).

[‡]We denote $g(n) = O(f(n))$ if there is a positive constant c_1 such that $\lim_{n\to\infty} \Pr\left(\frac{g(n)}{f(n)} \leq c_1\right) = 1$, and $g(n) = \Omega(f(n))$ if $f(n) = O(g(n))$. We also denote $g(n) = \Theta(f(n))$ if both $g(n) = O(f(n))$ and $g(n) = \Omega(f(n))$ hold.

6.6.6 Proof of Theorem 7

We first consider the case of $K_e > 0$. Based on Lemma 6, (6.16) can be rewritten as

$$\mathcal{F}_1(\mu) = \log_2\left[\frac{(1+K_e)(K_e - W_0)\sigma_e^2 L^{-\alpha}}{W_0\sigma_r^2\mu}\right];$$

$$\mathcal{F}_2(\nu) = \log_2\left[\frac{(1+K_e)(K_e - W_0)\sigma_e^2 L^{-\alpha}\nu}{W_0\sigma_r^2}\right],$$

which are obtained by substituting $\mu = {l_e}^{-\alpha_e}$ and $\nu = {l_e}^{\alpha_e}$. Hence, we have $\mathcal{F}_1(\mu) = \mathcal{F}_2(\nu)$.

For $\mathcal{F}_1(\mu)$, we can find that

$$\frac{\partial\mathcal{F}_1(\mu)}{\partial\mu} = -\frac{1}{\mu\ln 2} \leq 0;\ \frac{\partial^2\mathcal{F}_1(\mu)}{\partial\mu^2} = \frac{1}{\mu^2\ln 2} \geq 0.$$

$\mathcal{F}_1(\mu)$ is a monotonically decreasing and convex function of μ. Likewise, we can obtain

$$\frac{\partial\mathcal{F}_2(\nu)}{\partial\nu} = \frac{1}{\nu\ln 2} \geq 0;\ \frac{\partial^2\mathcal{F}_2(\nu)}{\partial\nu^2} = -\frac{1}{\nu^2\ln 2} \leq 0.$$

$\mathcal{F}_2(\nu)$ is a monotonically increasing and concave function of ν. By referring to (6.32) – (6.35) in the proof of Theorem 6, we have

$$\mathbb{E}_{l_e}\left[\mathcal{C}_{\text{out}}(L, l_e)\right] \approx \mathcal{C}_{\text{out}}\left(L, \bar{l}_e\right), \text{ if } K_e > 0. \tag{6.53}$$

In the case of $K_e = 0$, both the ϵ-outage secrecy rate, i.e.,

$$\mathcal{C}_{\text{out}}(L, l_e) = \log_2\left[\frac{\sigma_r^2\sigma_e^2 + \epsilon P\sigma_e^2 L^{-\alpha}}{\sigma_r^2\sigma_e^2 + (1-\epsilon)P\sigma_r^2 l_e^{-\alpha_e}}\right],$$

and the ergodic secrecy rate, i.e., $\mathcal{C}_{\text{erg}}(L, l_e)$, exhibit same monotonicity and concav-

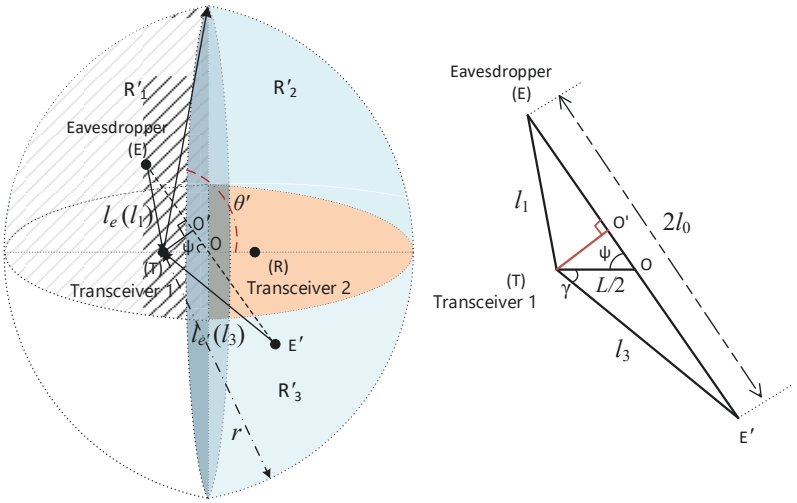


Figure 6.10 : Geometric interpretation for the evaluation of l_e

.

ity with regards to l_e. Based on the proof of Theorem 6, we have

$$\mathbb{E}_{l_e}\left[\mathcal{C}_{\text{out}}\left(L, l_e\right)\right] \approx \mathcal{C}_{\text{out}}\left(L, \bar{l}_e\right), \text{ if } K_e = 0. \tag{6.54}$$

By substituting $\bar{l}_e$ into (6.53) and (6.54), we can obtain (6.17). Also, the approximation error of (6.17) can asymptotically diminish with the increase of r and the number of antennas at the legitimate receiver and the eavesdropper, especially in the high SNR regime, as can be proved in the same way in Theorem 6. This concludes the proof of Theorem 7.

6.6.7 Proof of (6.23).

The expectation of the distance between the aerial eavesdropper to one of the ground transceivers can be evaluated by dividing the flight region into two subregions, i.e., Subregions R_1' and R_2', as shown in Fig. 6.10. Each of the subregions is half of a spherical cap centered at one of the transceivers. The distances from the eavesdropper inside the subregions to a ground transceiver can be separately evaluated. Without loss of generality, we evaluate the distances from the eavesdropper

to Transceiver 1, as follows.

When the eavesdropper is inside Subregion R_2', the volume of this half spherical cap can be evaluated to be $V_1 = \frac{\pi}{6}\left(2r^3 - \frac{3}{2}Lr^2 + \frac{L^3}{8}\right)$. The probability that the eavesdropper-transceiver distance l_e (denoted by l_2 in Subregion R_2') is shorter than τ is denoted by $\mathcal{P}'$ and equal to the probability that the eavesdropper is located within the spherical cap with the radius of τ. $\mathcal{P}' = \frac{16\tau^3 - 12L\tau^2 + L^3}{16r^3 - 12Lr^2 + L^3}$, $\frac{L}{2} \leq \tau \leq r$. The PDF of the eavesdropper-transceiver distance is given by

$$f_{l_2}(\tau) = \frac{48\tau^2 - 24L\tau}{16r^3 - 12Lr^2 + L^3}, \text{ if } \frac{L}{2} \leq \tau \leq r. \tag{6.55}$$

When the eavesdropper is inside Subregion R_1', we first plot the symmetric point of the eavesdropper with respect to Point O which is the halfway between the transceivers. The symmetric point, referred to as "virtual eavesdropper", is inside the virtual region symmetric to Subregion R_1' with respect to the ground plane. Given the uniform stationary distribution of the eavesdropper in Subregion R_2', the virtual eavesdropper also has a uniform stationary distribution in the virtual subregion R_3'. By using the cosine rule, we have

$$\cos\psi = \frac{(L/2)^2 + l_0^2 - l_1^2}{Ll_0}; \tag{6.56}$$

$$\cos(\pi - \psi) = \frac{(L/2)^2 + l_0^2 - {l_3}^2}{Ll_0}, \tag{6.57}$$

where l_1 is the distance between the eavesdropper inside Subregion R_1' and Transceiver 1; and l_3 is the distance between the virtual eavesdropper in the virtual subregion R_3' and the transceiver. l_3 has the exactly same PDF as l_2, due to the symmetry, i.e., $f_{l_3}(\tau) = \frac{48\tau^2 - 24L\tau}{16r^3 - 12Lr^2 + L^3}$, $\frac{L}{2} \leq \tau \leq r$.

Since $\cos\psi = -\cos(\pi - \psi)$, by separately adding and subtracting (6.56) and

(6.57), we can obtain

$$l_0 L\cos\psi = \frac{{l_3}^2 - {l_1}^2}{2}; \tag{6.58}$$

$${l_3}^2 + {l_1}^2 = 2l_0^2 + L^2/2. \tag{6.59}$$

According to the sine rule, we have

$$\frac{l_0}{\sin\gamma} = \frac{l_3}{\sin(\pi-\psi)}, \tag{6.60}$$

where $\gamma \in \left[0, \cos^{-1}\left(\frac{L}{2l_3}\right)\right]$ is the elevation angle between the virtual eavesdropper and the ground transmitter. γ is uniformly distributed within $\left[0, \cos^{-1}\left(\frac{L}{2l_3}\right)\right]$ given the uniform distribution of the eavesdropper in the 3D region. The PDF of γ conditioned on l_3 is $f_{\gamma|l_3}(x|\tau) = \frac{1}{\cos^{-1}\left(\frac{L}{2\tau}\right)}$. Therefore, the joint PDF of l_3 and γ can be given by

$$\begin{aligned} f_{l_3,\gamma}(\tau, x) &= f_{\gamma|l_3}(x|\tau)\cdot f_{l_3}(\tau) \\ &= \frac{1}{\cos^{-1}\left(\frac{L}{2\tau}\right)} \frac{48\tau^2 - 24L\tau}{16r^3 - 12Lr^2 + L^3}, \ \frac{L}{2} \le \tau \le r. \end{aligned} \tag{6.61}$$

Substitute (6.58) and (6.60) into $\sin^2\psi + \cos^2\psi = 1$,

$$l_0^2 = l_3^2\sin^2\gamma + \frac{\left(l_3^2 - l_1^2\right)^2}{4L^2}. \tag{6.62}$$

By substituting (6.62) into (6.59), we have

$$l_1^4 - 2\left(L^2 + l_3^2\right)l_1^2 + l_3^4 - 2L^2 l_3^2(1 - 2\sin^2\gamma) = 0. \tag{6.63}$$

By using the quadratic formula, we have $l_1^2 = L^2 + {l_3}^2 - 2Ll_3\cos\gamma$, since $l_1^2 = L^2 + {l_3}^2 + 2Ll_3\cos\gamma > l_3^2$ does not satisfy that $l_1 < l_3$ for $\psi \in \left[0, \frac{\pi}{2}\right]$. Therefore, we

have

$$l_1 = \sqrt{L^2 + {l_3}^2 - 2Ll_3 \cos\gamma},\ l_3 \in \left[\frac{L}{2}, r\right]. \tag{6.64}$$

By using (6.55), (6.61) and (6.64), we can obtain (6.23).

Chapter 7

Conclusion and Future Work

In summary, this thesis studies the coverage and capacity performance of UAV-enabled wireless networks. To improve network coverage and capacity, the UAV-enabled wireless network model is first established based on the different application scenarios of the UAV system. Then, the capacity and coverage performance, the secure coverage and capacity, under different scenarios have been studied and verified. The secrecy capacity performance of the terrestrial communication systems in the presence of aerial eavesdroppers have also been studied, and the impact of system parameters on network coverage and capacity has been theoretically analyzed. The detailed research work and contributions of this thesis are summarized as follows.

- In chapter 3, we analyzed the link capacity between autonomous UAVs with random 3D trajectories. Closed-form bounds for the capacity were derived between autonomous UAVs, and between UAVs and ground stations. The impact of network densification on the capacity, as well as the impacts of imperfect CSI and interference, were analyzed. Corroborated by simulations, our analysis showed that a U2U link with random 2D trajectories is superior to that with random 3D trajectories in terms of capacity due to its short average link distance. It was also revealed that a U2G link can incur substantially lower capacity than a U2U link even in the case that the 3D coverage of the UAVs is the same, as the result of its longer average link length.

- In chapter 4, we developed closed-form expressions for the outage probability of UAVs (or in other words, the one-hop connectivity of a UAV and the broadcast

connectivity of the UAV) in an uncoordinated UAV swarm, where the UAVs scoop within a 3D sphere with practical smooth turns both in the absence and presence of ground interference. Our analysis was based on comprehensive 3D geometric interpretations which ranslate the trajectories to steady-state spatial distributions of the UAVs. Extensive simulations confirm that our analyses are accurate and provide tight performance bounds for the connectivities of a dense uncoordinated UAV swarm in a large 3D space.

- In chapter 5, we proposed a novel trust model that can evaluate the reliability and security of UAV-enabled networks. The trust model was established based on UAVs' behaviors, the characteristics of channels between UAVs and the mobility of UAVs, which consists of four sections: the direct trust section, indirect trust section, integrated trust section, and trust update section. The concept of secure link in UAV-enabled networks was also presented on the basis of the proposed trust model, and it exists only when there is both a physical link and a trust link between two UAVs. In addition, both physical and secure connectivity probabilities between two UAVs in the presence of Doppler shift have been derived. Simulation results have shown that, compared to the physical connection probability with or without malicious attacks, the proposed trust model can effectively ensure secure communication and reliable connectivity between UAVs and enhance network performance when the UAV-enabled networks suffer malicious attacks and other security risks.

- In chapter 6, we analyzed the ergodic secrecy rate and the average ϵ-outage secrecy rate of a ground transmitter-receiver pair in the presence of an aerial eavesdropper flying a random trajectory in a 3D spherical region. Closed-form expressions were developed by exploiting the Jensen's inequality and Lambert W function, and validated by simulation results. Our analysis revealed that

the ground transmission is vulnerable to aerial eavesdropping which can be carried out in a distance without being noticed. 3D spherical regions were identified, within which the secrecy rates vanish.

The theoretical results obtained in this thesis provide new insights into the link capacity and connectivity (including secrecy capacity and connectivity) of UAV-enabled wireless networks in 3D spaces, and help compare diversity combining strategies in 3D fading channels. The "cut-off" density of the eavesdroppers under which the secrecy rates vanish was identified to help specify the "no-fly" zone to protect important infrastructure. However, due to time constraints, the relevant research content involved in this thesis has certain limitations. In the future, the follow-up research can be carried out from the following aspects:

1. Based on the theoretical analysis results of network coverage and capacity in this thesis, appropriate parameter optimization schemes, including the wireless parameters and flight parameters of UAVs, can be designed to achieve optimal network coverage and maximize network capacity. We will continue to pursue autonomous navigation and secure communication of UAVs by applying online learning techniques and our analytical results.

2. As an important part of the future 6G wireless communication system, the UAV system (or UAV systems) can serve as an effective relay node (or relay network) for information transfer between a terrestrial communication system and satellite communication system. Therefore, in future research work, we can investigate the architecture design of multi-layer networks, and then study the network performance of the multi-layer networks and the cooperation strategies and mechanisms between different layers of the system.

Bibliography

[1] S. A. Cambone, K. J. Krieg, P. Pace, and W. Linton, "Unmanned aircraft systems roadmap 2005-2030," *Office of the Secretary of Defense*, vol. 8, pp. 4–15, 2005.

[2] K. David and H. Berndt, "6G vision and requirements: Is there any need for beyond 5G?" *IEEE vehicular technology magazine*, vol. 13, no. 3, pp. 72–80, 2018.

[3] W. Saad, M. Bennis, and M. Chen, "A vision of 6g wireless systems: Applications, trends, technologies, and open research problems," *arXiv preprint arXiv:1902.10265*, 2019.

[4] B. Li, Z. Fei, and Y. Zhang, "UAV communications for 5G and beyond: Recent advances and future trends," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2241–2263, April 2019.

[5] Z. Feng, C. Qiu, Z. Feng, Z. Wei, W. Li, and P. Zhang, "An effective approach to 5G: Wireless network virtualization," *IEEE Communications Magazine*, vol. 53, no. 12, pp. 53–59, Dec. 2015.

[6] L. Gupta, R. Jain, and G. Vaszkun, "Survey of important issues in uav communication networks," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 2, pp. 1123–1152, Secondquarter 2016.

[7] T. Andre *et al.*, "Application-driven design of aerial communication networks," *IEEE Commun. Mag.*, vol. 52, no. 5, pp. 129–137, May 2014.

[8] K. Li, W. Ni, X. Wang, R. P. Liu, S. S. Kanhere, and S. Jha, "Energy-efficient cooperative relaying for unmanned aerial vehicles," *IEEE Trans. Mobile Comput.*, vol. 15, no. 6, pp. 1377–1386, Jun. 2016.

[9] M. Chen *et al.*, "Caching in the sky: Proactive deployment of cache-enabled unmanned aerial vehicles for optimized quality-of-experience," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 5, pp. 1046–1061, May 2017.

[10] S. Hayat, E. Yanmaz, and R. Muzaffar, "Survey on unmanned aerial vehicle networks for civil applications: A communications viewpoint," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 4, pp. 2624–2661, Fourthquarter 2016.

[11] G. Chmaj and H. Selvaraj, "Distributed processing applications for uav/drones: a survey," vol. 366, pp. 449–454, 2015.

[12] D. P. Watson and D. H. Scheidt, "Autonomous systems," *Johns Hopkins APL technical digest*, vol. 26, no. 4, pp. 368–376, 2005.

[13] I. Bekmezci, O. K. Sahingoz, and Ş. Temel, "Flying ad-hoc networks (fanets): A survey," *Ad Hoc Networks*, vol. 11, no. 3, pp. 1254–1270, 2013.

[14] J. Liu, Y. Shi, Z. M. Fadlullah, and N. Kato, "Space-Air-Ground integrated network: A survey," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 2714–2741, Fourthquarter 2018.

[15] N. Ahmed, S. S. Kanhere, and S. Jha, "Link characterization for aerial wireless sensor networks," in *2011 IEEE GLOBECOM Workshops (GC Wkshps)*, Dec. 2011, pp. 1274–1279.

[16] I. Guvenc, F. Koohifar, S. Singh, M. L. Sichitiu, and D. Matolak, "Detection, tracking, and interdiction for amateur drones," *IEEE Commun. Mag.*, vol. 56, no. 4, pp. 75–81, Apr. 2018.

[17] T. Sosnowski, G. Bieszczad, H. Madura, and M. Kastek, "Thermovision system for flying objects detection," in *Baltic URSI Symposium (URSI)*, May 2018, pp. 141–144.

[18] E. Sakhaee and A. Jamalipour, "The global in-flight internet," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 9, pp. 1748–1757, 2006.

[19] E. Sakhaee, A. Jamalipour, and N. Kato, "Aeronautical ad hoc networks," in *IEEE Wireless Communications and Networking Conference (WCNC)*, vol. 1. IEEE, 2006, pp. 246–251.

[20] C. Qiu, Z. Wei, Z. Feng, and P. Zhang, "Joint resource allocation, placement and user association of multiple UAV-mounted base stations with in-band wireless backhaul," *IEEE Wireless Communications Letters*, vol. 8, no. 6, pp. 1575–1578, Dec. 2019.

[21] E. W. Frew and T. X. Brown, "Airborne communication networks for small unmanned aircraft systems," *Proceedings of the IEEE*, vol. 96, no. 12, 2008.

[22] E. Baccarelli and A. Fasano, "Some simple bounds on the symmetric capacity and outage probability for qam wireless channels with rice and nakagami fadings," *IEEE J. Sel. Areas Commun.*, vol. 18, no. 3, pp. 361–368, Mar. 2000.

[23] P. Yang, Y. Wu, and H. Yang, "Capacity of nakagami- m fading channel with bpsk/qpsk modulations," *IEEE Commun. Lett.*, vol. 21, no. 3, pp. 564–567, Mar. 2017.

[24] Z. Rezki and M. S. Alouini, "On the capacity of nakagami-m fading channels with full channel state information at low snr," *IEEE Wireless Commun. Lett.*, vol. 1, no. 3, pp. 253–256, Jun. 2012.

[25] X. Li, X. Chen, J. Zhang, Y. Liang, and Y. Liu, "Capacity analysis of α-η-κ-μ fading channels," *IEEE Commun. Lett.*, vol. PP, no. 99, pp. 1–1, Jun. 2017.

[26] W. Ni, M. Abolhasan, B. Hagelstein, R. P. Liu, and X. Wang, "A new trellis model for mac layer cooperative retransmission protocols," *IEEE Trans. Veh. Tech.*, vol. 66, no. 4, pp. 3448–3461, 2017.

[27] B. Hagelstein, M. Abolhasan, D. Franklin, F. Safaei, and W. Ni, "Analytic performance model for state-based mac layer cooperative retransmission protocols," *IEEE Trans. on Mobile Comput.*, vol. 15, no. 1, pp. 32–44, 2016.

[28] A. N. Hong *et al.*, "Channel capacity analysis of indoor environments for location-aware communications," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Dec. 2016, pp. 1–6.

[29] Z. Wei, H. Wu, X. Yuan, S. Huang, and Z. Feng, "Achievable capacity scaling laws of three-dimensional wireless social networks," *IEEE Trans. Veh. Technol.*, vol. 67, no. 3, pp. 2671–2685, Mar. 2018.

[30] Z. Wei, Z. Feng, X. Yuan, X. Feng, Q. Zhang, and X. Wang, "The achievable capacity scaling laws of 3D cognitive radio networks," in *IEEE ICC*, May 2016, pp. 1–6.

[31] S. Chandrasekharan *et al.*, "Designing and implementing future aerial communication networks," *IEEE Commun. Mag.*, vol. 54, no. 5, pp. 26–34, May 2016.

[32] A. Merwaday, A. Tuncer, A. Kumbhar, and I. Guvenc, "Improved throughput coverage in natural disasters: Unmanned aerial base stations for public-safety communications," *IEEE Veh. Technol. Mag.*, vol. 11, no. 4, pp. 53–60, 2016.

[33] C. Qiu, Z. Wei, X. Yuan, Z. Feng, and P. Zhang, "Multiple UAV-mounted base stations placement and user association with joint fronthaul and backhaul optimization," *IEEE Transactions on Communications*, 2019.

[34] C. Qiu, Z. Wei, Z. Feng, and P. Zhang, "Backhaul-aware trajectory optimization of fixed-wing UAV-mounted base station for continuous available wireless service," *IEEE Access*, 2019.

[35] V. Sharma, M. Bennis, and R. Kumar, "Uav-assisted heterogeneous networks for capacity enhancement," *IEEE Commun. Lett.*, vol. 20, no. 6, pp. 1207–1210, 2016.

[36] M. Mozaffari, W. Saad, M. Bennis, and M. Debbah, "Efficient deployment of multiple unmanned aerial vehicles for optimal wireless coverage," *IEEE Commun. Lett.*, vol. 20, no. 8, pp. 1647–1650, 2016.

[37] I. Y. Abualhaol and M. M. Matalgah, "Outage probability analysis in a cooperative uavs network over nakagami-m fading channels," in *Proc. IEEE Vehicular Technology Conf. (VTC)*, Sept. 2006, pp. 1–4.

[38] ——, "Performance analysis of multi-carrier relay-based uav network over fading channels," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Dec. 2010, pp. 1811–1815.

[39] K. An, M. Lin, and T. Liang, "On the performance of multiuser hybrid satellite-terrestrial relay networks with opportunistic scheduling," *IEEE Commun. Lett.*, vol. 19, no. 10, pp. 1722–1725, Oct. 2015.

[40] J. S. Yan, C. Q. Hua, C. L. Chen, and X. P. Guan, "The capacity of aeronautical ad-hoc networks," *Wireless networks*, vol. 20, no. 7, pp. 2123–2130, 2014.

[41] Y. Wang *et al.*, "Throughput and delay of single-hop and two-hop aeronautical communication networks," *J. Commun. Netw.*, vol. 17, no. 1, pp. 58–66, Feb. 2015.

[42] P. K. Sharma and D. I. Kim, "Coverage probability of 3D UAV networks with RWP Mobility-based altitude control," in *IEEE ICC Workshops*, May 2018, pp. 1–6.

[43] V. V. Chetlur and H. S. Dhillon, "Downlink coverage analysis for a finite 3-D wireless network of unmanned aerial vehicles," *IEEE Trans. Commun.*, vol. 65, no. 10, pp. 4543–4558, Oct. 2017.

[44] L. Kong and G. Kaddoum, "On physical layer security over the Fisher-Snedecor $\mathcal{F}$ wiretap fading channels," *IEEE Access*, vol. 6, pp. 39 466–39 472, 2018.

[45] B. He, X. Zhou, and A. L. Swindlehurst, "On secrecy metrics for physical layer security over quasi-static fading channels," *IEEE Trans. Wireless Commun.*, vol. 15, no. 10, pp. 6913–6924, Oct. 2016.

[46] S. Vuppala, Y. J. Tolossa, G. Kaddoum, and G. Abreu, "On the physical layer security analysis of hybrid millimeter wave networks," *IEEE Trans. Commun.*, vol. 66, no. 3, pp. 1139–1152, Mar. 2018.

[47] D. S. Karas, A. A. Boulogeorgos, and G. K. Karagiannidis, "Physical layer security with uncertainty on the location of the eavesdropper," *IEEE Wireless Commun. Lett.*, vol. 5, no. 5, pp. 540–543, Oct. 2016.

[48] Y. Ai, M. Cheffena, A. Mathur, and H. Lei, "On physical layer security of double rayleigh fading channels for vehicular communications," *IEEE Wireless Commun. Lett.*, pp. 1–1, 2018.

[49] G. Zhang, Q. Wu, M. Cui, and R. Zhang, "Securing UAV communications via joint trajectory and power control," *arXiv preprint arXiv:1801.06682*, 2018.

[50] A. Li, Q. Wu, and R. Zhang, "Uav-enabled cooperative jamming for improving secrecy of ground wiretap channel," *arXiv preprint arXiv:1801.06841*, 2018.

[51] Q. Wang, Z. Chen, W. Mei, and J. Fang, "Improving physical layer security using UAV-enabled mobile relaying," *IEEE Wireless Commun. Lett.*, vol. 6, no. 3, pp. 310–313, Jun. 2017.

[52] H. Lee, S. Eom, J. Park, and I. Lee, "UAV-aided secure communications with cooperative jamming," *IEEE Trans. Veh. Technol.*, vol. 67, no. 10, pp. 9385–9392, Oct. 2018.

[53] Y. Cai, F. Cui, Q. Shi, M. Zhao, and G. Y. Li, "Dual-UAV-enabled secure communications: Joint trajectory design and user scheduling," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 9, pp. 1972–1985, Sep. 2018.

[54] Y. Zhu, G. Zheng, and M. Fitch, "Secrecy rate analysis of UAV-enabled mmwave networks using matérn hardcore point processes," *IEEE J. Sel. Areas Commun.*, pp. 1–1, 2018.

[55] C. Liu, T. Q. S. Quek, and J. Lee, "Secure UAV communication in the presence of active eavesdropper (invited paper)," in *2017 9th International Conference on Wireless Communications and Signal Processing (WCSP)*, Oct. 2017, pp. 1–6.

[56] M. Cui, G. Zhang, Q. Wu, and D. W. K. Ng, "Robust trajectory and transmit power design for secure UAV communications," *IEEE Trans. Veh. Technol.*, vol. 67, no. 9, pp. 9042–9046, Sept. 2018.

[57] J. Ye, C. Zhang, H. Lei, G. Pan, and Z. Ding, "Secure UAV-to-UAV systems with spatially random UAVs," *IEEE Wireless Commun. Lett.*, pp. 1–1, 2018.

[58] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inform. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[59] J. Xie, Y. Wan, J. H. Kim, S. Fu, and K. Namuduri, "A survey and analysis of mobility models for airborne networks," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1221–1238, Third Quarter 2014.

[60] Y. Wan, K. Namuduri, Y. Zhou, and S. Fu, "A smooth-turn mobility model for airborne networks," *IEEE Trans. Veh. Technol.*, vol. 62, no. 7, pp. 3359–3370, Sept. 2013.

[61] M. M. Azari, F. Rosas, K. C. Chen, and S. Pollin, "Ultra reliable uav communication using altitude and cooperation diversity," *IEEE Trans. Commun.*, vol. 66, no. 1, pp. 330–344, Jan. 2018.

[62] D. B. Da Costa and S. Aïssa, "Capacity analysis of cooperative systems with relay selection in nakagami-m fading," *IEEE Commun. Lett.*, vol. 13, no. 9, 2009.

[63] M. Z. Bocus, C. P. Dettmann, and J. P. Coon, "An approximation of the first order marcum q-function with application to network connectivity analysis," *IEEE Commun. Lett.*, vol. 17, no. 3, pp. 499–502, 2013.

[64] N. B. Rached, A. Kammoun, M. S. Alouini, and R. Tempone, "Unified importance sampling schemes for efficient simulation of outage capacity over generalized fading channels," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 2, pp. 376–388, Mar. 2016.

[65] S.-Y. Chung, G. D. Forney, T. J. Richardson, and R. Urbanke, "On the design of low-density parity-check codes within 0.0045 db of the shannon limit," *IEEE Commun. Lett.*, vol. 5, no. 2, pp. 58–60, 2001.

[66] M. Crofton, *Probability, in Encyclopaedia Britannica*, 9th ed. Britannica Inc., 1885.

[67] M. M. Azari, H. Sallouha, A. Chiumento, S. Rajendran, E. Vinogradov, and S. Pollin, "Key technologies and system trade-offs for detection and localization of amateur drones," vol. 56, no. 1, pp. 51–57, Jan. 2018.

[68] M. Mayer and I. Molchanov, "Limit theorems for the diameter of a random sample in the unit ball," *Extremes*, vol. 10, no. 3, pp. 129–150, 2007.

[69] I. S. Gradshteyn and I. M. Ryzhik, *Table of integrals, series, and products*, 7th ed. Academic press, 2000.

[70] E. W. Frew and T. X. Brown, "Airborne communication networks for small unmanned aircraft systems," *Proceedings of the IEEE*, vol. 96, no. 12, 2008.

[71] W. Saad, Z. Han, T. Basar, M. Debbah, and A. Hjorungnes, "A selfish approach to coalition formation among unmanned air vehicles in wireless networks," in *Proc. Int. Conf. Game Theory for Networks (Gamenets)*, May 2009, pp. 259–267.

[72] M. Mozaffari, W. Saad, M. Bennis, and M. Debbah, "Unmanned aerial vehicle with underlaid device-to-device communications: Performance and tradeoffs," *IEEE Trans. Wireless Commun.*, vol. 15, no. 6, pp. 3949–3963, 2016.

[73] M. M. Azari, F. Rosas, A. Chiumento, and S. Pollin, "Coexistence of terrestrial and aerial users in cellular networks," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Dec. 2017.

[74] B. V. D. Bergh, A. Chiumento, and S. Pollin, "Lte in the sky: trading off propagation benefits with interference costs for aerial nodes," *IEEE Commun. Mag.*, vol. 54, no. 5, pp. 44–50, May 2016.

[75] E. Baccarelli and M. Biagi, "Error resistant space-time coding for emerging 4g-wlans," in *Wireless Communications and Networking, 2003. WCNC 2003. 2003 IEEE*, vol. 1. IEEE, 2003, pp. 72–77.

[76] ——, "Performance and optimized design of space-time codes for mimo wireless systems with imperfect channel estimates," *IEEE trans. signal processing*, vol. 52, no. 10, pp. 2911–2923, 2004.

[77] W. M. Gifford, M. Z. Win, and M. Chiani, "Diversity with practical channel estimation," *IEEE Trans. Wireless Commun.*, vol. 4, no. 4, pp. 1935–1947, 2005.

[78] A. Nuttall, "Some integrals involving the q_m function (corresp.)," *IEEE Trans. Inform. Theory*, vol. 21, no. 1, pp. 95–96, 1975.

[79] Y. Sun, Á. Baricz, and S. Zhou, "On the monotonicity, log-concavity, and tight bounds of the generalized marcum and nuttall q-functions," *IEEE Trans. Inform. Theory*, vol. 56, no. 3, pp. 1166–1186, 2010.

[80] M. Kuczma, *An introduction to the theory of functional equations and inequalities: Cauchy's equation and Jensen's inequality.* Springer Science & Business Media, 2009.

[81] S. Kandeepan, K. Gomez, L. Reynaud, and T. Rasheed, "Aerial-terrestrial communications: terrestrial cooperation and energy-efficient transmissions to aerial base stations," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 50, no. 4, pp. 2715–2735, October 2014.

[82] K. Govindan and P. Mohapatra, "Trust computations and trust dynamics in mobile adhoc networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 2, pp. 279–298, Second 2012.

[83] Z. Movahedi, Z. Hosseini, F. Bayan, and G. Pujolle, "Trust-distortion resistant trust management frameworks on mobile ad hoc networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 2, pp. 1287–1309, 2016.

[84] G. Han, J. Jiang, L. Shu, J. Niu, and H.-C. Chao, "Management and applications of trust in wireless sensor networks: A survey," *J. Comput.and Syst. Sci.*, vol. 80, no. 3, pp. 602–617, 2014.

[85] J. Jiang, G. Han, F. Wang, L. Shu, and M. Guizani, "An efficient distributed trust model for wireless sensor networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 5, pp. 1228–1237, 2015.

[86] H. Xia, Z. Jia, and E. H. . Sha, "Research of trust model based on fuzzy theory in mobile ad hoc networks," *IET Inform. Secur.*, vol. 8, no. 2, pp. 88–103, March 2014.

[87] G. Han, J. Jiang, L. Shu, and M. Guizani, "An attack-resistant trust model based on multidimensional trust metrics in underwater acoustic sensor network," *IEEE Trans. Mobile Comput.*, vol. 14, no. 12, pp. 2447–2459, Dec. 2015.

[88] M. K. Simon and M.-S. Alouini, *Digital communication over fading channels.* John Wiley & Sons, 2005, vol. 95.

[89] A. Josang, "An algebra for assessing trust in certification chains," in *Proceedings of the Network and Distributed Systems Security Symposium (NDSS). The Internet Society*, 1999.

[90] J. Vazifehdan, R. V. Prasad, and I. Niemegeers, "Energy-efficient reliable routing considering residual energy in wireless ad hoc networks," *IEEE Trans. Mobile Comput.*, vol. 13, no. 2, pp. 434–447, 2014.

[91] E. Elnahrawy and B. Nath, "Cleaning and querying noisy sensors," in *Proceedings of the 2nd ACM international conference on Wireless sensor networks and applications*. ACM, 2003, pp. 78–87.

[92] H.-S. Lim, Y.-S. Moon, and E. Bertino, "Provenance-based trustworthiness assessment in sensor networks," in *Proceedings of the Seventh International Workshop on Data Management for Sensor Networks*. ACM, 2010, pp. 2–7.

[93] M. Salmanian, P. C. Mason, J. Treurniet, J. Hu, L. Pan, and M. Li, "A modular security architecture for managing security associations in MANETs," in *The 7th IEEE International Conference on Mobile Ad-hoc and Sensor Systems (IEEE MASS)*. IEEE, 2010, pp. 525–530.

[94] K. Wang and M. Wu, "A trust approach for node cooperation in MANET," in *International Conference on Mobile Ad-Hoc and Sensor Networks*. Springer, 2007, pp. 481–491.

[95] R. Janaswamy, "Angle of arrival statistics for a 3D spheroid model," *IEEE Trans. veh. technol.*, vol. 51, no. 5, pp. 1242–1247, 2002.

[96] I. S. Gradshteyn and I. M. Ryzhik, *Table of integrals, series, and products*, 7th ed. Academic press, 2000.

[97] H. Li, B. Yang, C. Chen, and X. Guan, "Connectivity of aeronautical ad hoc networks," in *Proc. IEEE Globecom Workshops (GC Wkshps)*. IEEE, 2010, pp. 1788–1792.

[98] F. Jameel, S. Wyne, G. Kaddoum, and T. Q. Duong, "A comprehensive survey on cooperative relaying and jamming strategies for physical layer security," *IEEE Commun. Surveys Tuts.*, pp. 1–1, 2018.

[99] S. Vuppala and G. Kaddoum, "Secrecy capacity analysis in D2D underlay cellular networks: Colluding eavesdroppers," in *IEEE PIMRC*, Oct. 2017, pp. 1–7.

[100] E. M. Royer, P. M. Melliar-Smith, and L. E. Moser, "An analysis of the optimum node density for ad hoc mobile networks," in *IEEE ICC*, vol. 3, Jun. 2001, pp. 857–861 vol.3.

[101] E. Kuiper and S. Nadjm-Tehrani, "Geographical routing with location service in intermittently connected MANETs," *IEEE Tran. Veh. Technol.*, vol. 60, no. 2, pp. 592–604, Feb 2011.

[102] W. Wang, X. Guan, B. Wang, and Y. Wang, "A novel mobility model based on semi-random circular movement in mobile ad hoc networks," *Information Sciences*, vol. 180, no. 3, pp. 399–413, 2010.

[103] A. Tiwari *et al.*, "Mobility aware routing for the airborne network backbone," in *Proc. Military Commun. Conf.*, Nov. 2008, pp. 1–7.

[104] A. Al-Hourani, S. Kandeepan, and S. Lardner, "Optimal lap altitude for maximum coverage," *IEEE Wireless Commun. Lett.*, vol. 3, no. 6, pp. 569–572, Dec. 2014.

[105] B. Sklar, "Rayleigh fading channels in mobile digital communication systems .I. characterization," *IEEE Commun. Mag.*, vol. 35, no. 7, pp. 90–100, Jul. 1997.

[106] X. Yu, J. Zhang, M. Haenggi, and K. B. Letaief, "Coverage analysis for millimeter wave networks: The impact of directional antenna arrays," *IEEE J. Sel. Areas in Commun.*, vol. 35, no. 7, pp. 1498–1512, July 2017.

[107] P. Révész, *The laws of large numbers*. Academic Press, 2014, vol. 4.

[108] P. Billingsley, *Convergence of probability measures*. John Wiley & Sons, 2013.

[109] Z. Feng, L. Ji, Q. Zhang, and W. Li, "Spectrum management for mmwave enabled UAV swarm networks: Challenges and opportunities," *IEEE Commun. Mag.*, vol. 57, no. 1, pp. 146–153, Jan. 2019.

[110] C. Zhang, W. Zhang, W. Wang, L. Yang, and W. Zhang, "Research challenges and opportunities of UAV millimeter-wave communications," *IEEE Wireless Commun.*, vol. 26, no. 1, pp. 58–62, Feb. 2019.